



The ONE!

One Schedule to Rule them All!

Welcome to the "One Schedule to Rule them All!". Thank you for your interest by using this. This is an attempt to make things easier for you, the DEF CON attendee, to figure out the when/what/where during the chaos of DEF CON 34.

It started out simple. I had a Kindle and wanted an ebook of the schedule so I didn't have to wear out the paper pamphlet by pulling it out after every talk to figure out where to go next. Back then there was only the main DEF CON tracks, not really any Villages, and production of the ebooks were easy. Over time the Village system developed with a resulting multiplication in complexity, both for attendees and for my production. The offerings no longer include epub and mobi formats and instead now include html, csv, PDF, ical, public Google calendar, and mysql dump format files. Hopefully you'll find something of use.

The intent is still to be a resource to answer the question at the end of an hour of "What's next?"

As a general rule I do not include:

- Off-site events
- Blatent vender pitch events
- DEF CON events are emphasized, so BSides Las Vegas and BlackHat tend to not show up

Be sure to check out the Links section at the bottom of this. Most all of the events listed here were derived from these links and a Infoboot data feed. There is much more going on at DEF CON than what is listed here.

Check out the Guides/Tips/FAQs links if you're new to Las Vegas.

Notable suggestions are:

- Bring comfortable shoes, you'll be doing a lot more walking than you expect
- Bring a water bottle to keep hydrated
- Beware of going out doors, there's nothing like LV sun and heat
- Everything in Las Vegas is a longer walk than you think
- Relax, don't try to see everything, you'll never be able to!
- Have FUN!

And finally, this is only as good as the ideas and information used to generate it. I welcome your constructive suggestions and comments. Please send them to qumqats@outel.org

Have a good time at DEF CON 34!

Index of DEF CON 34 Activities

[Maps List](#)

[Maps Browser](#)

[Detailed Creator/Village Info](#)

[Creator/Villages Table](#)

Hour by Hour list of happenings, start at the top, or go to a specific day.

[Schedule](#)

[- Thursday](#) - [Friday](#) - [Saturday](#) - [Sunday](#)

Sorted list of all the Speakers Names linked to their talk's description.

[Speaker List](#)

Sorted list of all the Talk's titles linked to the talk description.

[Talk Title List](#)

Talk lists for each Creator/Village, start at the alphabetic top, or go to a specific Creator/Village.

[Creator/Village Talk List](#)

[.EDU Community](#) - [Adversary Village](#) - [Aerospace Village](#) - [AI Village](#) - [AppSec Village](#) - [Biohacking Village](#) - [Blacks In Cyber Village](#) - [Blue Team Village](#) - [Bug Bounty Village](#) - [Call Center Village](#) - [Car Hacking Village](#) - [Cloud Village](#) - [CodeBloom](#) - [Contests](#) - [Crypto & Privacy Village](#) - [Cryptocurrency Village](#) - [Data Duplication Village](#) - [DCNextGen](#) - [DEF CON Groups](#) - [DEF CON Talks](#) - [DEF CON Training](#) - [DEF CON Workshops](#) - [Demo Labs](#) - [Embedded Systems Village](#) - [Game Hacking Village](#) - [Hackers.town](#) - [Ham Radio Village](#) - [ICS Village](#) - [IoT Village](#) - [La Villa Community](#) - [Lockpick Village](#) - [Lonely Hackers Club](#) - [Maker's Village](#) - [Malware Village](#) - [Maritime Hacking Village](#) - [Middle Easterns & Africans in Cyber Security \(MEACS\)](#) - [Misc](#) - [Mobile Hacking Community](#) - [Nix Vegas Community](#) - [Noob Community](#) - [OSINT For Good Community](#) - [OWASP Foundation](#) - [Packet Hacking Village](#) - [Payment Village](#) - [Physical Security Village](#) - [Policy @ DEF CON](#) - [Quantum Village](#) - [Queercon Community](#) - [Radio Frequency Village](#) - [Recon Village](#) - [Red Team Village](#) - [Scambait Village](#) - [Social Engineering Community Village](#) - [Social Gatherings/Events](#) - [Telecom Village](#) - [The Diana Initiative](#) - [Voting Village](#) -

Descriptions and Info for all the talks.

[Talk Descriptions](#)

Contests Table

[Contests](#)

Demolabs Table

[Demolabs](#)

Workshops Table

[Workshops](#)

Paid Trainings Table

[Paid Trainings](#)

Parties, Gatherings, and Events Table

[Parties Gatherings Events](#)

DEF CON 34 Vendors
[Vendors](#)

DEF CON 34 Exhibitors
[Exhibitors](#)

DEF CON 34 Communities
[Communities](#)

The latest news from defcon.org
[DEF CON News](#)

The answer to your questions about DEF CON overall.
[DEF CON FAQ](#)

[DEF CON .org Links](#)

[Combined Schedule Sources](#)

[Interesting Links](#)

[Guides/Tips/FAQs](#)

Maps List

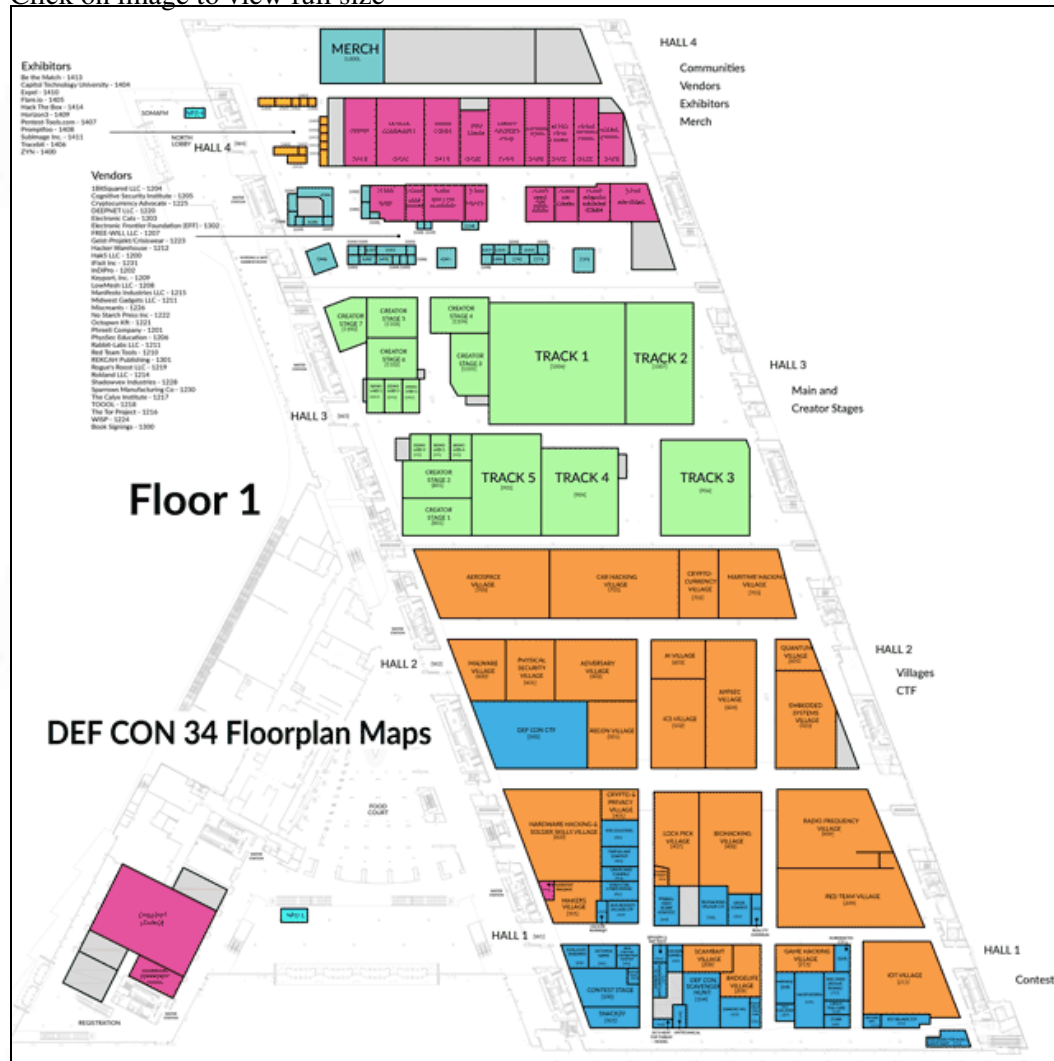
Overview of the area around DEF CON 34

[Click on image to view full size](#)



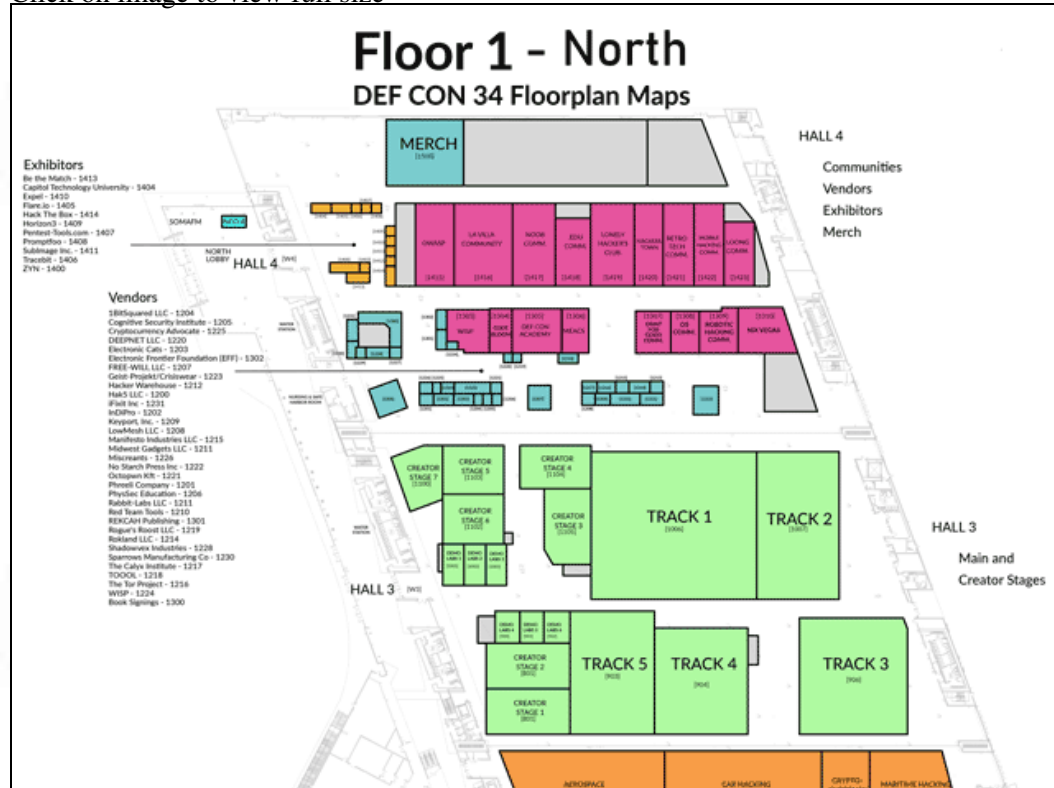
LVCCW Full map of Level 1

[Click on image to view full size](#)



LVCCW map of North portion of Level 1

[Click on image to view full size](#)

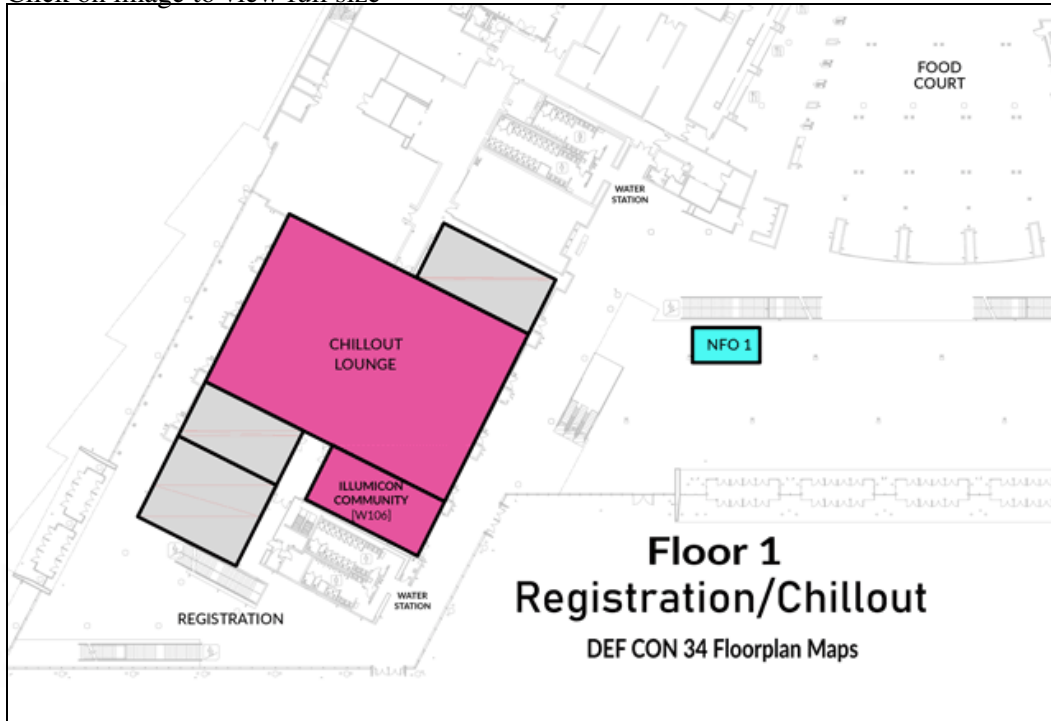


[Click on image to view full size](#)



LVCCW map of South Lobby and Registration Area of Level 1

[Click on image to view full size](#)



LVCCW map of Hall 1 of Level 1

[Click on image to view full size](#)



LVCCW map of Hall 2 of Level 1

Click on image to view full size

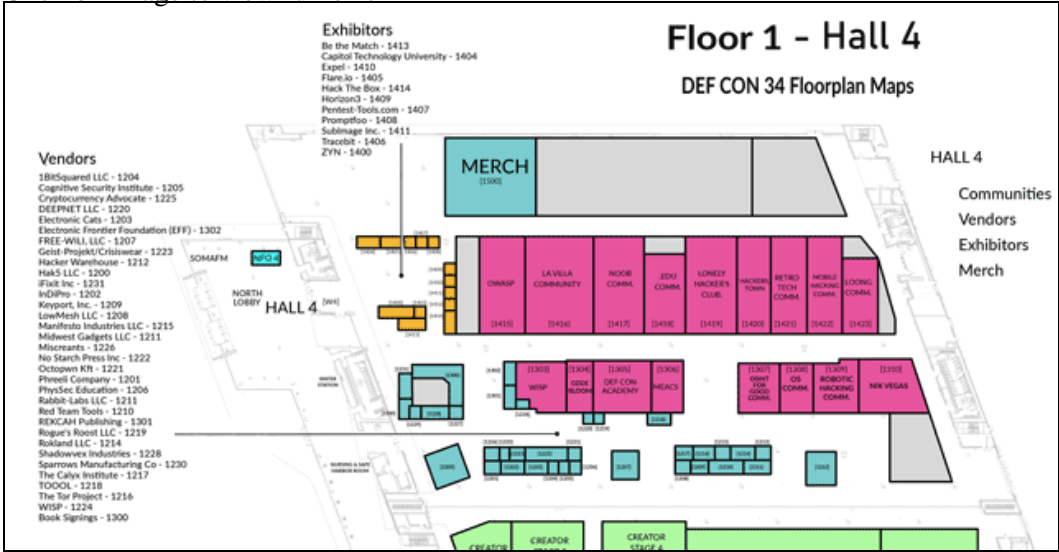


LVCCW map of Hall 3 of Level 1

[Click on image to view full size](#)

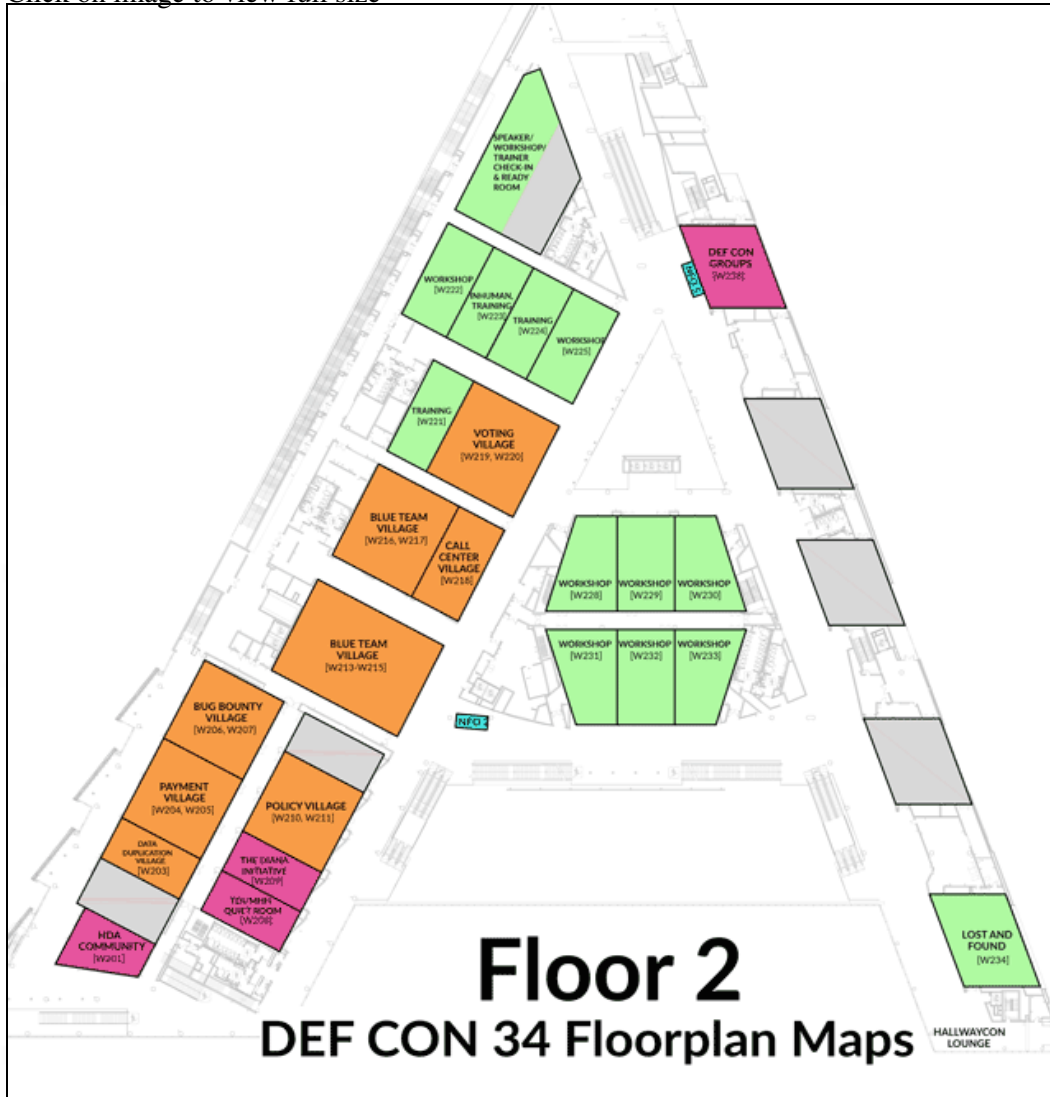


[Click on image to view full size](#)

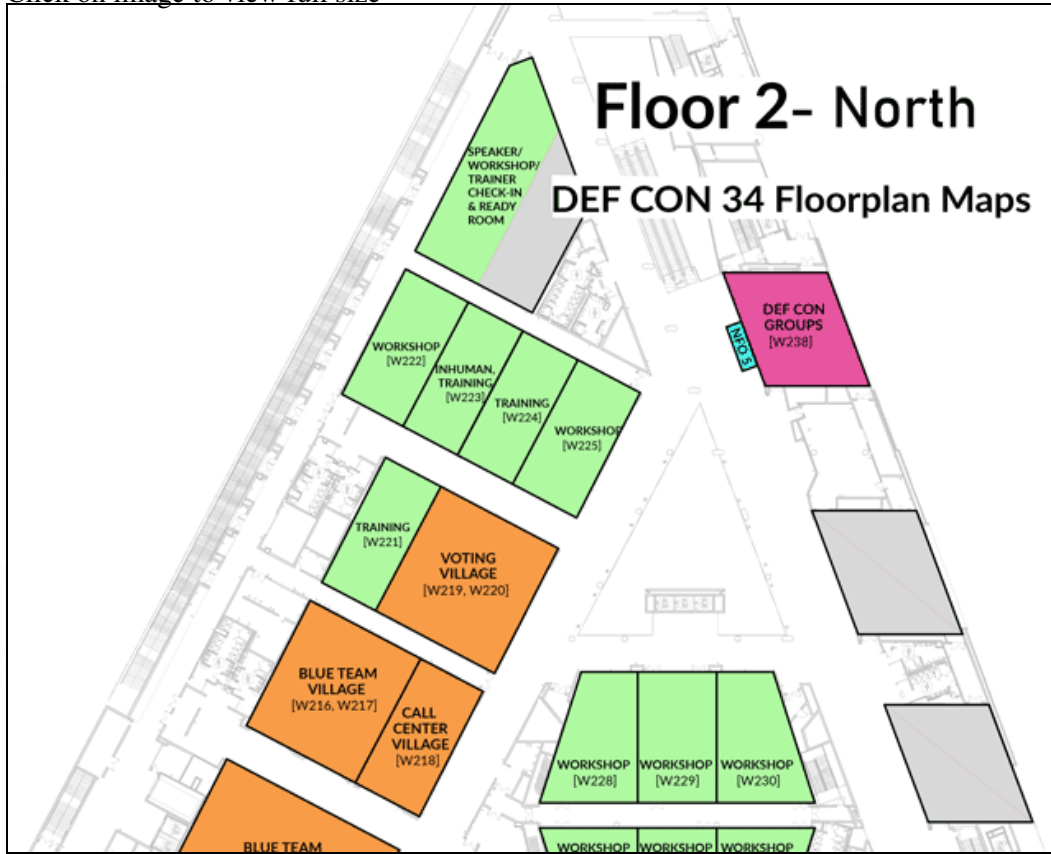


LVCCW Full map of Level 2

[Click on image to view full size](#)

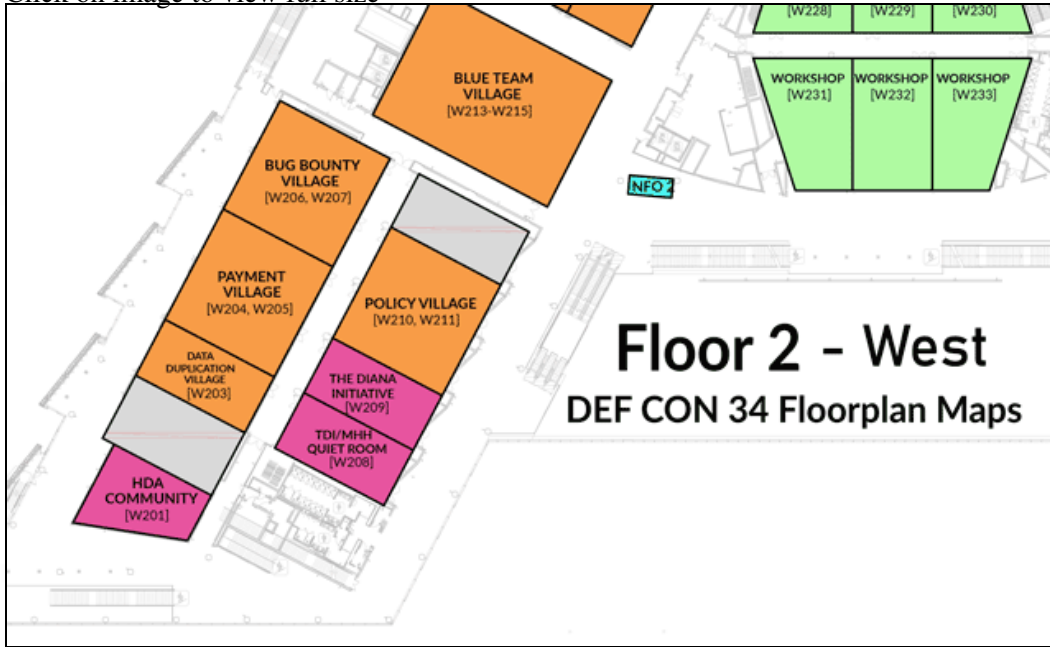


[Click on image to view full size](#)



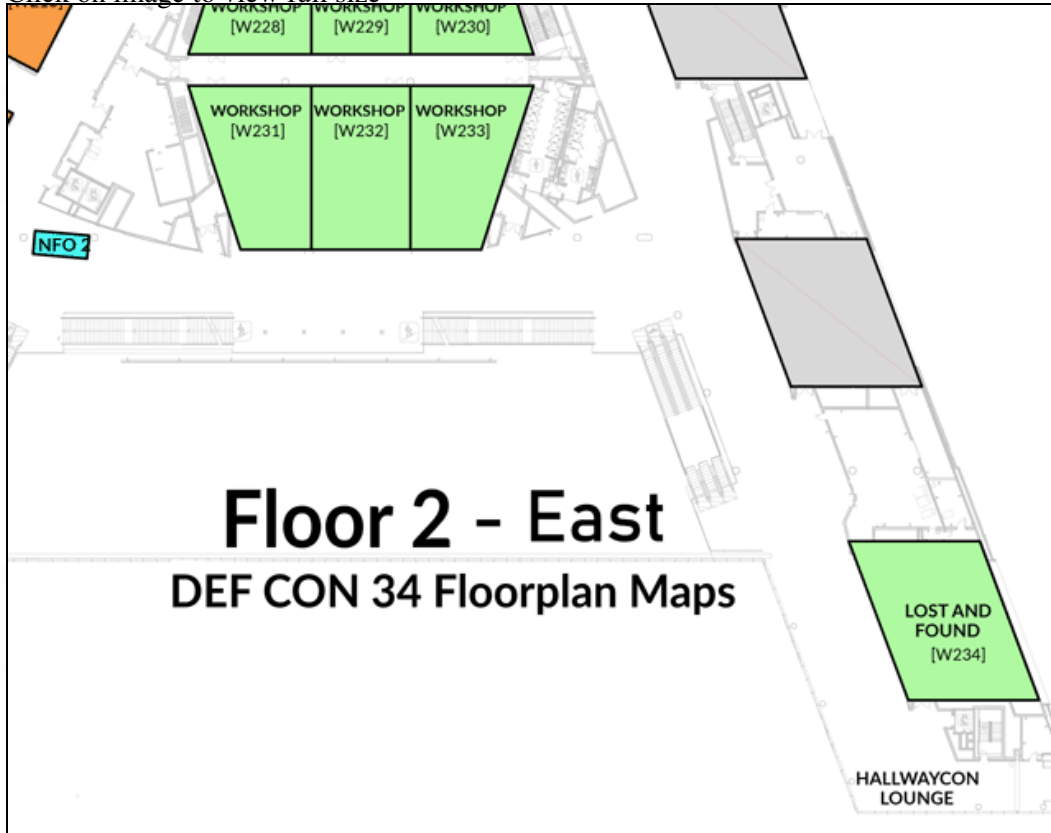
LVCCW map of West portion of Level 2

[Click on image to view full size](#)



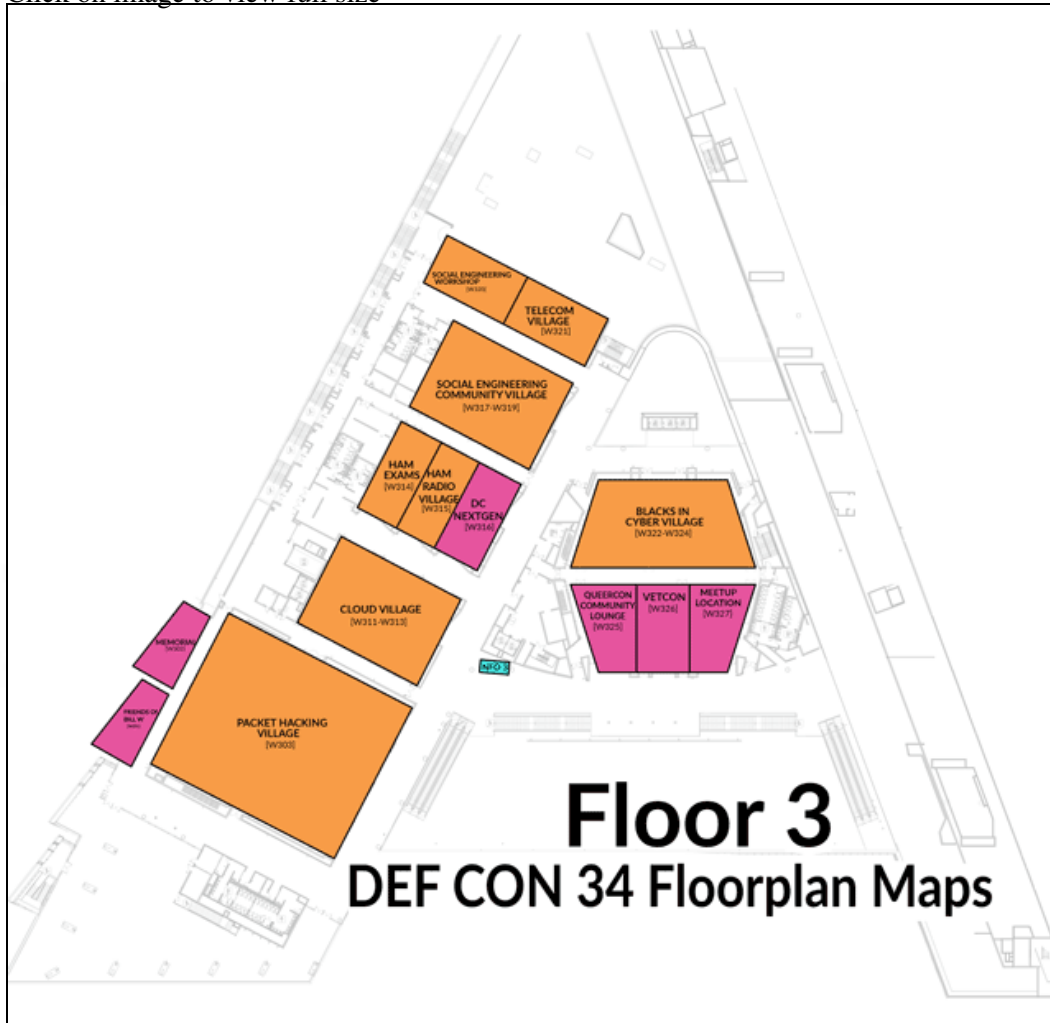
LVCCW map of East portion of Level 2

[Click on image to view full size](#)

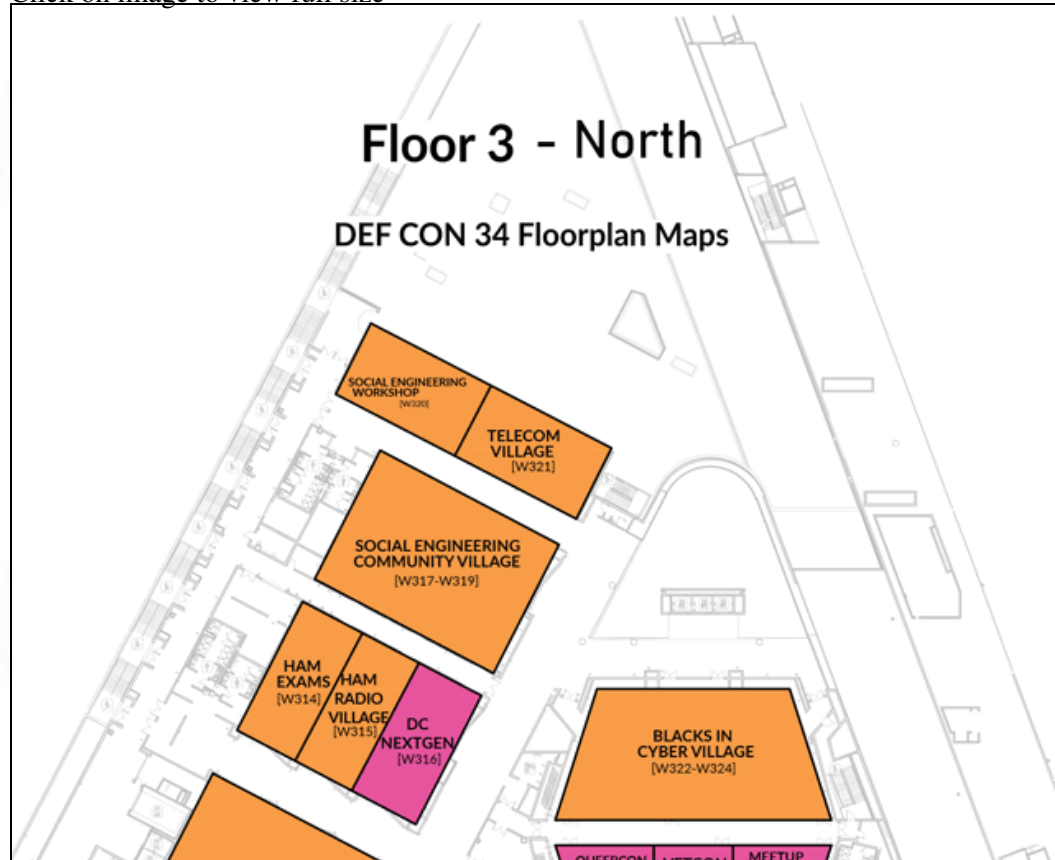


LVCCW Full map of Level 3

[Click on image to view full size](#)

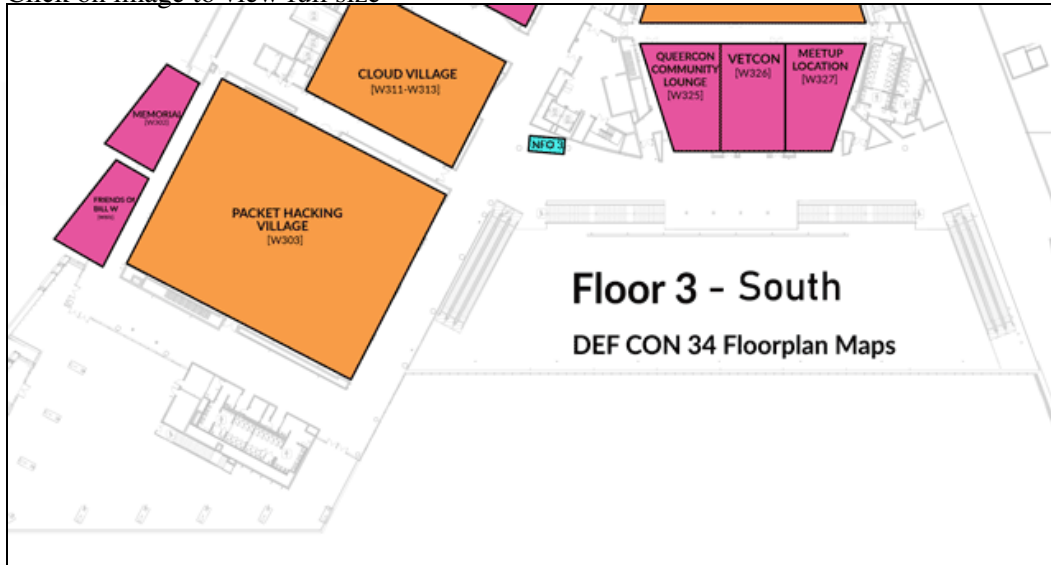


[Click on image to view full size](#)



LVCCW map of South portion of Level 3

[Click on image to view full size](#)



Pool Parties - Sahara

[Click on image to view full size](#)



Map Browser

[LV Strip Overview - Closeup - Sahara](#)

[LVCCW_L1_Full - L1_North - L1_South](#)

[L1_Reg - L1_Hall1 - L1_Hall2 - L1_Hall3 - L1_Hall4](#)

[LVCCW_L2_Full - L2_North - L2_West - L2_East](#)

[LVCCW_L3_Full - L3_North - L3_South](#)

[One page DEF CON 34 map](#)

[Las Vegas Convention Center - Virtual Tour](#)



Detailed Creator/Village Info

Adversary Village

Adversary Village: [Talk List](#)

Home Page: <https://adversaryvillage.org>

Sched Page: <https://adversaryvillage.org/adversary-events/DEFCON-34/schedule/>

DC Village Page: https://defcon.org/html/defcon-34/dc-34-villages.html#orga_40719

Location: LVCCW Level 1 Hall 2 602 (Adversary Village) - [Map](#)

Social Media Links:

TW [@AdversaryVillag](#)

<https://defcon.social/@AdversaryVillage>

YT <https://youtube.com/AdversaryVillage>

DC <https://discord.gg/GDB3rC7KYz>

TI [@AdversaryVillage](#)

FB [@AdversaryVillage](#)

LI [@adversaryvillage](#)



Adversary Village is a community initiative focused on adversary simulation, emulation, offensive cyber security, purple teaming, and adversary tradecraft. The village explores how real adversaries operate, how offensive capabilities are built and deployed, and how nation state sponsored threat actors continue to shape the modern cyber threat landscape.

Our focus spans adversary and APT simulation, ransomware and breach emulation, adversarial attack simulation, supply chain security, adversary intelligence, research on nation state threat actors, hacker survival skills and the broader adversarial mindset. If it involves thinking and operating like an adversary, pull up a chair, that's a conversation we want to have.

The goal of Adversary Village is to build an open and collaborative security community where researchers, practitioners, and organizations can come together to develop and share new approaches to adversary simulation and emulation. Understanding how adversaries think and operate is essential to building stronger defenses.

At the village, the community will experience deep technical workshops, live demonstrations, panel discussions, adversary emulation labs, breach simulation exercises, CTFs, and other hands on activities. Everything is designed to give participants

practical exposure to adversarial operations while encouraging collaboration and knowledge sharing across the security community.

Links:

Website - <https://adversaryvillage.org>

Mastodon (@AdversaryVillage@defcon.social) - <https://defcon.social/@AdversaryVillage>

[Return to Index](#)

AI Village

AI Village: [Talk List](#)

Home Page: <https://aivillage.org/>

DC Village Page: https://defcon.org/html/defcon-34/dc-34-villages.html#orga_40718

Location: LVCCW Level 1 Hall 2 603 (AI Village) - [Map](#)

Social Media Links:

TW [@aivillage_dc](#)

TI [@aivillage](#)

YT [link](#)

DC <https://discord.com/invite/GX5fhfT>

LI [@aivillage](#)



We're bringing AI Village back to focus on what actually matters: practical, no-bullshit AI security. LLMs are an amazing technology, but they're not magic. We are stripping away the industry hype and focusing on hands-on skills, whether you are building your first exploit or leading an AI red team.

Here is what you can expect this year:

Drop-In Workshops: Walk up, grab a seat, and learn. We have drop in hands on mini-workshops on a bunch of topics. These include basic AI topics like how LLMs actually work, and how to build agents from scratch. For red teamers we have ones ranging from prompt injection to manipulating malware detection models. This is all running locally on a cluster we're bringing to DEF CON.

HalCTF: Our main competition this year will teach you how to write and fine-tune your own pentesting agent using open-source models. To handle the massive compute load, we're safely detonating these agents on GCP, giving each participant a dedicated GPU for their models.

Other Agent Shenanigans: The field moves fast and there's going to be something new by defcon. We're bringing a lot of compute to host things and we'll have some surprises in the space.

Whether you want to hear top-tier research from the people actually breaking these models or you just want to sit down and write an autonomous pentesting agent, we have the hardware and the labs ready for you.

Links:

Website - <https://aivillage.org/>

[Return to Index](#)

AppSec Village

AppSec Village: [Talk List](#)

Home Page: <https://www.appsecvillage.com/>

Sched Page: <https://www.appsecvillage.com/events/dc-2026>

DC Village Page: https://defcon.org/html/defcon-34/dc-34-villages.html#orga_40721

Location: LVCCW Level 1 Hall 2 604 (Appsec Village) - [Map](#)

Social Media Links:

TW [@AppSec_Village](#)

LI [@appsecvillage](#)

YT <https://www.youtube.com/c/AppSecVillage>

DC <https://discord.gg/5XY8qYXd7R>



The AppSec Village is a 100% volunteer-run creator space at DEF CON where hackers learn how modern software gets broken and how to make it harder to break. Expect attacker-minded talks and live demos, plus hands-on workshops and Practical On-Demand sessions where you can practice techniques with the community, from finding and exploiting vulnerabilities to fixing them correctly. You can also explore the village Arsenal for rapid demos of open-source AppSec

tools, and compete in the Fix the Flag wargame, a CTF-style contest that rewards you for remediating vulnerabilities and hardening an app before turning to offense. If software is your target or your craft, you will leave with practical skills, tools, and mental models you can use immediately.

Prerequisites

For talks, panels, and tool demos, there are no prerequisites, and no special equipment is needed. For hands-on activities (workshops, some Practical On-Demand sessions, and the Fix the Flag wargame), bringing a laptop is strongly recommended so you can follow along and run tools. No specialized hardware is required, and any session-specific setup notes will be provided by the activity owner ahead of time.

Links:

Website - <https://www.appsecvillage.com/>

Mastodon (@AppSecVillage@defcon.social) - <https://defcon.social/@AppSecVillage>

[Return to Index](#)

Aerospace Village

Aerospace Village: [Talk List](#)

Home Page: <https://aerospacevillage.org/>

DC Village Page: https://defcon.org/html/defcon-34/dc-34-villages.html#orga_40720

Location: LVCCW Level 1 Hall 2 700 (Aerospace Village) - [Map](#)

Social Media Links:

TW [@secureaerospace](#)

LI [@aerospace-village](#)

TW [@hack_a_sat](#)

DC <https://discord.gg/gV4EWuk>

YT <https://www.youtube.com/c/AerospaceVillage>

<https://defcon.social/@aerospacevillage>



The aviation and space industries, security researchers, and the public share a common goal: safe, reliable, and trustworthy aviation and space operations. For too long, negative perceptions and fractured trust on all sides have held back collaboration between the aviation, space, and security researcher communities that has advanced safety, reliability, and security of other industries. As the traditional domains of aviation safety and cybersecurity increasingly overlap, more effective collaboration between stakeholders ensures we will be safer, sooner, together. Through the Aerospace Village, the security research community invites industry leaders, researchers and academia interested in aviation and space security, safety, and resilience to attend, understand, collaborate together to achieve our common goals. Empathy and understanding build common ground, while acts and words likely to increase division between these two communities undermine these efforts. The Aerospace Village welcomes those who seek to improve aviation and space security, safety, and resilience through positive, productive collaboration among all ecosystem stakeholders.

Our Goal

The Aerospace Village is a volunteer team of hackers, pilots, and policy advisors who come from the public and private sectors. We believe the flying public deserves safe, reliable, and trustworthy air travel which is highly dependent on secure aviation and space operations.

Links:

Website - <https://aerospacevillage.org>

Mastodon (@aerospacevillage@defcon.social) - <https://defcon.social/@aerospacevillage>

[Return to Index](#)

Bug Bounty Village

Bug Bounty Village: [Talk List](#)

Home Page: <https://bugbountydefcon.com/>

Sched Page: <https://www.bugbountydefcon.com/agenda-2026>

DC Village Page: https://defcon.org/html/defcon-34/dc-34-villages.html#orga_40726

Location: LVCCW Level 2 W206-207 (Bug Bounty Village) - [Map](#)

Social Media Links:

TW [@BugBountyDEFCON](#)

YT <https://www.youtube.com/BountyTalks>

TW [@arl_rose](#)

TW [@infinitelogins](#)

YT <https://www.youtube.com/infinitelogins>

IG [@bugbountydefcon](#)



Welcome to the Bug Bounty Village at DEF CON, the central hub for the global community of bug bounty hunters, security researchers, and hackers. Now in our third year, we are returning to DEF CON bigger and better than ever.

Hacking is at the core of everything we do. Whether you are a newcomer looking to submit your first report or a seasoned veteran chasing critical exploits, our space offers the tools, community support, and technical insights you need to level up. Attendees can expect a high-energy environment filled with technical talks, hands-on workshops, and live hacking challenges. Following the massive success of our inaugural CTF in 2025—which drew over 750 participants—we are expanding our competitive offerings to push your skills to the limit.

Visit us and participate in our custom electronic badges giveaways, get an exclusive challenge coin, and engage with some of the world's most prolific bug bounty hunters. You will learn everything from the ""obvious"" essentials—like setting up a secure testing environment—to cutting-edge techniques for breaking complex modern systems. If you want to see how the world's most impactful bugs are found, fixed, and rewarded, this is the place to be.

Prerequisites:

To fully participate in any of the workshops, trainings, and / or CTF, attendees should bring a laptop and a charger. For the safety of your hardware and personal data, it is a prerequisite that all participants have their laptops configured for the DEF CON Wi-Fi in a secure manner prior to joining village activities.

While the village offers content for all experience levels, a foundational understanding of web protocols and a curious, analytical mindset will help you get the most out of our hands-on challenges. Those interested in the CTF may want to brush up on common web vulnerability classes and basic scripting to hit the ground running.

Links:

Website - <https://www.bugbountydefcon.com/>

[Return to Index](#)

Biohacking Village

Biohacking Village: [Talk List](#)

Home Page: <https://www.villageb.io/>

Sched Page: <https://www.villageb.io/Labs>

DC Village Page: https://defcon.org/html/defcon-34/dc-34-villages.html#orga_40723

Location: LVCCW Level 1 Hall 1 408 (Biohacking Village) - [Map](#)

Social Media Links:

TW [@dc_bhv](#)

LI [@biohacking-village](#)

YT <http://youtube.com/biohackingvillage>

TI [@biohackingvillage](#)

DC <https://discord.gg/Q8ubDb5>

<https://bsky.app/profile/villageb.io>
[link](#)



Biohacking Village (BHV) is DEF CON's hands-on home for hacking the systems that keep humans alive. We bring a hacker lens to healthcare, medical devices, and the messy reality where firmware, networks, clinical workflows, and cybersecurity collide. If you like breaking things to understand them - BHV is your stop.

At BHV, attendees don't just watch talks. They do the work: crack open artifacts, follow packets, unravel bad assumptions, and learn how vulnerabilities show up in real clinical contexts. Our creator space is built like a lab-meets-playground: part training ground, part CTF arena, part community hub- where beginners get a friendly on-ramp and experienced researchers get puzzles that bite back.

Healthcare is critical infrastructure, and medical devices are computers with unique constraints: safety requirements, legacy environments, weird protocols, long lifecycles, and a threat surface that spans from embedded firmware to cloud dashboards to the humans using them. BHV translates that complexity into hacker-accessible challenges, with clear rules-of-engagement and responsible research guardrails.

The Biohacking Village:

- Treats healthcare tech as a systems hacking problem, not a niche specialty
- Turns real-world failure modes into repeatable labs and CTF challenges
- Brings together hackers, engineers, clinicians, and policy folks for cross-pollination you don't get

anywhere else - Teaches not only “how to break it,” but also how to document, disclose, and improve it

Who BHV is for:

- Beginners who want a welcoming first step into hardware/firmware, medical tech, and embedded research - Experienced hackers who want high-signal challenges and healthcare-specific nuance - Builders and defenders who want to understand the attacker mindset without compromising safety

Come by Biohacking Village if you want to learn real skills, meet a community that’s equal parts brilliant and helpful, and explore one of the most consequential targets in security: healthcare.

Prerequisites

- ◊ A laptop (Windows/Mac/Linux) that can run a VM or containers
- ◊ USB-A/USB-C adapters (because the dongle life chose us)
- ◊ Basic comfort with 'terminal stuff' helps, but we'll have ramps for beginners
- ◊ Hacking Tools

Links:

Website - <https://villageb.io>

[Return to Index](#)

Blacks In Cyber Village

Blacks In Cyber Village: [Talk List](#)

Home Page: <https://www.blacksincyberconf.com/bic-village>

Sched Page: <https://www.blacksincyberconf.com/bic-village>

DC Village Page: https://defcon.org/html/defcon-34/dc-34-villages.html#orga_40724

Location: LVCCW Level 3 W322-W324 (BIC Village) - [Map](#)

Social Media Links:

TW [@BlackInCyberCo1](#)

<https://defcon.social/@blacksincyber>

TI [@blacksincybersecurity](#)

YT [link](#)

LI [@blackincyberconference](#)

PT [@blacksincybersecurity](#)

FB [@blackincyberconf](#)



The Blacks In Cybersecurity (B.I.C.) Village seeks to bring culturally diverse perspectives to the holistic Cybersecurity community; by way of a series of talks and a capture the flag event. In providing these activities, we hope to help highlight Black experiences, innovations in the field, Black culture and educate the community about Black history.

In doing this, we believe that we can better educate and normalize the discussion of deficiency or prejudices in Cybersecurity education/development for minority communities. We also believe this effort can be translated to aid in eradication of these issues in the Cybersecurity and Hacker/Maker community and allow for more diverse hobbyists and professionals to engage and contribute.

Prerequisites

Laptop, Tablet

Links:

Mastodon (@blacksincyber@infosec.exchange) - <https://infosec.exchange/@blacksincyber>

Website - <https://www.blacksincyberconf.com/bic-village>

Mastodon (@blacksincyber@defcon.social) - <https://defcon.social/@blacksincyber>

[Return to Index](#)

Badgelife Village

Badgelife Village: [Talk List](#)

Home Page: <https://badge.life/>

Sched Page: <https://badge.life/>

DC Village Page: https://defcon.org/html/defcon-34/dc-34-villages.html#orga_41349

Location: LVCCW Level 1 Hall 1 209 (Badgelife Village) - [Map](#)

Social Media Links:

<https://reanimationxp.bsky.social/>

<https://github.com/badgelife/website>

DC <https://discord.gg/R4jGhTqJ3J>



You asked for it and we're back again! The Badgelife Village (formerly Community) is a proper home for all things Badgelife on the con floor! Visit us to experience the Badgelife Museum, featuring hundreds of current and past community-made badges, SAOs, MiniBadges and more! Donate your own badges and SAOs you've made or collected to the museum, and see them come back to con year after year.. or bring what you've got to trade with the community via our ""take-one, leave-one"" SAO Trading Wall! Attend our in-person Badge Trading meetups to swap badges you've already enjoyed for new creations!

If you're interested in creating Badges or SAOs yourself, we will have lots of interesting badge creators around showing off their work and giving training in the form of talks and workshops on their methodologies. Come learn from the best and meet your favorite creators at our various Badgemaker Meetups! Before and after con, visit our village at <https://badge.life>, where we're kicking off our online Badge Archive. Closer to con we'll post our schedule for any con workshops, talks or activities on the site as well, so check there for our meetup times and events. Hope to see you at the village!

Links:

reanimationxp.bsky.social - <https://reanimationxp.bsky.social>
Website - <https://badge.life>

[Return to Index](#)

Blue Team Village

Blue Team Village: [Talk List](#)

Home Page: <https://blueteamvillage.org/>

Sched Page: <https://btv-dc34.sessionize.com/schedule/day/20260807>

DC Village Page: https://defcon.org/html/defcon-34/dc-34-villages.html#orga_40725

Location: LVCCW Level 2 W213-217 (Blue Team Village) - [Map](#)

Social Media Links:

TW [@BlueTeamVillage](#)

TI [@blueteamvillage](#)

YT <https://www.youtube.com/c/blueteamvillage>

DC <https://discord.gg/blueteamvillage>

<https://defcon.social/@blueteamvillage>



Welcome to the other side of the hacking mirror. Blue Team Village (BTV) is both a place and a community built for and by people who defend computer systems, networks, and people against cyber attacks. It's a place to gather, talk, share, and learn from each other about the latest tools, technologies, and tactics that our community can use to detect attackers and prevent them from achieving their goals.

Links:

Website - <https://blueteamvillage.org>

blueteamvillage.bsky.social - <https://blueteamvillage.bsky.social>

[Return to Index](#)

Call Center Village

Call Center Village: [Talk List](#)

Home Page: <https://www.callcentervillage.com/>

Sched Page: <https://www.callcentervillage.com/events>

DC Village Page: https://defcon.org/html/defcon-34/dc-34-villages.html#orga_41429

Location: LVCCW Level 2 W218 (Call Center Village) - [Map](#)

Social Media Links:

<https://defcon.social/@callcentervillage>

<https://github.com/callcentervillage>



Security teams have spent years hardening web-apps, email-gateways, and network-perimeters. Meanwhile, the phone line sitting on every receptionist's desk remains almost completely unmonitored. Nobody's deploying a firewall between a caller and the person who picks up. Caller ID authentication has made some progress, but the conversation itself? Wide open.

And now that AI-generated voices can pass for the real thing and automated agents are handling account resets and payment processing, that gap is getting a lot more interesting. Call Center Village is where voice security, conversational AI, and social engineering collide — across both voice and text channels.

Sit down at a workstation and synthesize a copy of your own voice with open-source tools running on a local GPU, or let our staff walk you through the process. Dig into voice pipelines, deepfake audio detection, and the arms race between the two. Wire up a working conversational AI agent — stitching together the real-time audio infrastructure, transcription, language model, and speech synthesis that make these systems speak.

On the text side, go after chatbot agents tasked with handling simulated customer interactions. Find the cracks in their system prompts, hijack conversation logic, and convince them to do things their developers never intended. Once you're ready, muster all your skills to take on our Escalation Desk CTF, the official Call Center Village contest at DEF CON 34.

We've also got a collection of vintage telephones, prank extensions, chatty AI-agents, and a British-style telephone booth worth stopping by for.

No prior experience required. If you know how to make a phone call or type a message, you're already qualified. Equipment is provided, including laptops and ANC headsets - but you're more than welcome to bring your own devices.

Links:

Website - <https://www.callcentervillage.com>

Mastodon (@callcentervillage@defcon.social) - <https://defcon.social/@callcentervillage>

[Return to Index](#)

CodeBloom

CodeBloom: [Talk List](#)

Home Page: <https://codebloom.org/>

Social Media Links:

<https://mastodon.social/@codebloom>

<https://bsky.app/profile/codebloom.bsky.social>

IG [@codebloomhq](#)

FB [@profile.php?id=61584968176159](#)

[Return to Index](#)

Cryptocurrency Village

Cryptocurrency Village: [Talk List](#)

Home Page: <https://www.cryptocurrencyvillage.cc/>

Sched Page: <https://www.cryptocurrencyvillage.cc/village/>

DC Village Page: https://defcon.org/html/defcon-34/dc-34-villages.html#orga_41359

Location: LVCCW Level 1 Hall 2 702 (Cryptocurrency Village) - [Map](#)



They told us blockchains were immutable, trustless, autonomous. Like a fortress of math and consensus. But every protocol hides a human fingerprint where math has edge cases, and consensus can be forked.

At the Cryptocurrency Village, we don't just read the whitepaper — we set it on fire. You'll discover how financial technology really works: by breaking it. Learn the unique ways cryptocurrency systems are attacked, defended, and secured. Whether you are looking to audit smart contracts, track illicit funds across chains, or analyze the cryptographic primitives powering decentralized networks, the Cryptocurrency Village offers a deep dive into the unique intersection of economics, math, and offensive security.

Win prizes in the Cryptocurrency Challenge, colocated within the village walls. Workshops and competitions provide a safe workspace and give the experience of mentored participation in a well equipped and comfortable environment. Visit the hackathon floor to witness teams building strange new financial tools, breaking assumptions, and pushing hardware and

software beyond their intended limits.

From curious newcomers asking their first questions to seasoned cryptohackers hunting new exploits and allies, the Cryptocurrency Village is a meeting point for those drawn to the intersection of money, code, cryptography, and rebellion. It is a place to interrogate the financial systems that increasingly govern freedom, privacy, ownership, and trust itself. Get inspired to explore cryptocurrency where practical finance hacking for the public good is encouraged — even while wearing the red team jersey.

We inclusively welcome all cryptocurrency projects and their cousins across adjacent cryptographic and decentralized technology communities. Come hack with us. The testnet vault is waiting, and we've already left the door unlocked!

Links:

Mastodon (@cryptocurrency@defcon.social) - <https://defcon.social/@cryptocurrency>

Website - <https://www.cryptocurrencyvillage.cc/>

[Return to Index](#)

Car Hacking Village

Car Hacking Village: [Talk List](#)

Home Page: <https://www.carhackingvillage.com/>

Sched Page: <https://www.carhackingvillage.com/defcon-34-talks>

DC Village Page: https://defcon.org/html/defcon-34/dc-34-villages.html#orga_40727

Location: LVCCW Level 1 Hall 2 701 (Car Hacking Village) - [Map](#)

Social Media Links:

<https://x.com/CarHackVillage>

YT <http://youtube.com/@carhackingvillage>

LI [@car-hacking-village](#)

DC <https://discord.gg/zz7xUPZcre>

<https://github.com/car-hacking-village>



The Car Hacking Village is the primary hub for the global community dedicated to securing over a billion vehicles. For DEF CON 34, we move beyond theory and put you directly into the driver's seat of modern exploitation. This year's experience is built around raw, hands-on access to live vehicle architectures and hardware benches. Whether you're intercepting CAN bus traffic in real-time or probing wireless entry points, you'll be working with the same systems used by top researchers. We've curated a high-intensity environment where you can tear down ECUs, bypass security gateways, and collaborate to dismantle the latest threats facing the industry.

Prerequisites

To participate effectively in the Car Hacking Village at DEF CON 34, attendees should bring a laptop with multiple USB ports (or appropriate adapters) and a functional Linux environment. We do not provide specialized tools on-site, so you'll need to bring your own—such as a USB-to-CAN adapter (e.g., Canable, ValueCAN), a SDR (e.g., RTL-SDR, HackRF), or a multimeter—is encouraged for independent exploration.

Knowledge of the Linux command line and basic Python is highly recommended. For those looking to hit the ground running, we suggest brushing up on CAN bus fundamentals and basic reverse engineering of binary data. Familiarity with tools like Wireshark and can-utils will allow you to dive straight into the live vehicle architectures.

Links:

Website - <https://www.carhackingvillage.com/>

[Return to Index](#)

Cloud Village

Cloud Village: [Talk List](#)

Home Page: <https://cloud-village.org/>

Sched Page: <https://www.cloud-village.org/dc34>

DC Village Page: https://defcon.org/html/defcon-34/dc-34-villages.html#orga_40728

Location: LVCCW Level 3 W311-W313 (Cloud Village) - [Map](#)

Social Media Links:

https://x.com/cloudvillage_dc

YT https://www.youtube.com/cloudvillage_dc

DC <https://discord.com/invite/p3S3KVD2Tp>

LI [@cloudvillage-dc](#)

FB [@1DVeGSw5KT](#)

IG [@cloudvillage_dc](#)



Cloud Village is an open space to meet folks interested in offensive and defensive aspects of cloud security. The village helps security professionals understand evolving threats, implement best practices and defend against real-world cloud vulnerabilities via Talks, Labs, Panels and a continuous two-day Cloud Security focussed CTF.

Our CTF will be a jeopardy-style, two-day competition (Friday and Saturday) focused on real-world cloud security. Participants will tackle challenges centered around securing, exploiting, and analyzing cloud environments across major platforms including AWS, GCP, and Azure. The contest will feature scenarios involving IAM misconfigurations, container and Kubernetes security, cloud reconnaissance, infrastructure exploitation, logging and detection, serverless security, secrets management, and cloud-native attack paths. Teams will test their skills across offensive and defensive cloud security domains while competing for prizes awarded to the top 3 teams.

Prerequisites

- ◇ Come with an open mind and zeal to learn as a group.
- ◇ For Labs and CTF, please bring a laptop with admin right and unfiltered internet access.

Links:

Mastodon (@cloudvillage_dc@mastodon.social) - https://mastodon.social/@cloudvillage_dc

Website - <https://www.cloud-village.org/>

[Return to Index](#)

Contests

Contests: [Talk List](#)

Home Page: <https://defcon.outel.org/dcwp/dc34/activities/c/>

Social Media Links:

[link](#)

[Return to Index](#)

Crypto & Privacy Village

Crypto & Privacy Village: [Talk List](#)

Home Page: <https://cryptovillage.org/>

Sched Page: <https://cryptovillage.org/cpv-13/>

DC Village Page: https://defcon.org/html/defcon-34/dc-34-villages.html#orga_40729

Location: LVCCW Level 1 Hall 1 401 (Crypto & Privacy Village) - [Map](#)

Social Media Links:

TW [@cryptovillage](#)

SL <https://cryptovillage.slack.com/>

YT [link](#)

TI [@cryptovillage](#)

<https://defcon.social/@cryptovillage>



Launched in 2014, Crypto & Privacy Village (CPV) is a community-run village centred on privacy and cryptography that aims to educate and inform the general public, students, educators, hackers, security and privacy professionals, and policymakers. We provide a unique hybrid space that features talks; chill space for relaxing with friends, doing CTFs, and cross industry networking; the Gold Bug Challenge and desk for hints and support; privacy-related art installations; and an information desk for questions about privacy and cryptography. Come talk with us about facial recognition technology, privacy enhancing clothing, or crypto backdoor laws!

Prerequisites

We will provide make up but it would be better for attendees to bring their own if possible (to see how effective they are); laptops and notebooks for the Gold Bug and other activities (we will provide paper)

Links:

Mastodon (@cryptovillage@defcon.social) - <https://defcon.social/@cryptovillage>

Website - <https://cryptovillage.org>

[Return to Index](#)

DEF CON Groups

DEF CON Groups: [Talk List](#)

[Return to Index](#)

DEF CON Talks

DEF CON Talks: [Talk List](#)

Home Page: <https://defcon.outel.org/dcwp/dc34/activities/dctalks/>

Social Media Links:

TW [@defcon](#)

FB [@defcon](#)

YT <https://www.youtube.com/user/DEFCONConference>

<http://www.reddit.com/r/defcon>

IG [@wearedefcon](#)

DC <https://discord.gg/defcon>

[Return to Index](#)

DEF CON Workshops

DEF CON Workshops: [Talk List](#)

Home Page: <https://defcon.outel.org/dcwp/dc34/activities/workshops/>

[Return to Index](#)

Data Duplication Village

Data Duplication Village: [Talk List](#)

Home Page: <https://dcddv.org/>

Sched Page: <https://dcddv.org/dc34-talks-schedule>

DC Village Page: https://defcon.org/html/defcon-34/dc-34-villages.html#orga_40730

Location: LVCCW Level 2 W203 (Data Duplication Village) - [Map](#)

Social Media Links:

TW [@DDV_DC](#)



Data Duplication Village

The Data Duplication Village has all the updated bits and bytes available from infocon.org packed up into nice, neat packages. If you're looking for a copy of just about any security con talk known to hacker-kind, a copy of the VX-Underground archive, hash tables or those elusive rainbow tables, you'll find them here. Our village provides a "free-to-you" service of providing you with direct access to terabytes of useful data to help build those hacking skills and allow open discussions with others.

We also encourage DC Next Gen participation to ensure that our future generations have the opportunity to explore the details of how past and current data storage works!

Links:

Website - <https://dcdv.org>

[Return to Index](#)

Demo Labs

Demo Labs: [Talk List](#)

Home Page: <https://defcon.ouel.org/dcwp/dc34/activities/dl/>

[Return to Index](#)

DCNextGen

DCNextGen: [Talk List](#)

Home Page: <https://dcnextgen.org/>

Social Media Links:

<https://defcon.social/@defconnextgen>

[Return to Index](#)

Embedded Systems Village

Embedded Systems Village: [Talk List](#)

Home Page: <https://embeddedvillage.org/>

DC Village Page: https://defcon.org/html/defcon-34/dc-34-villages.html#orga_40731

Location: LVCCW Level 1 Hall 2 503 (Embedded Systems Village) - [Map](#)

Social Media Links:

TW [@EmbeddedVillage](#)



Embedded Systems Village (ESV) is a community of enthusiastic hackers who love working with hardware. Run by Hacking Villages Inc., a US-based 501(c)3 nonprofit, ESV's mission is to educate attendees on how embedded systems work, how to analyze their hardware components, how to identify vulnerabilities, and how to prevent cyberattacks on these systems.

Everything ESV does is grounded in real embedded devices — occasionally jamming a whole bunch of concepts onto a single piece of hardware, but always with an authentic real-world analog. Whether you're walking in for the first time or you've been hacking hardware for years, ESV provides a challenging yet supportive environment to hack, learn, and innovate.

Prerequisites:

- Attendees wishing to compete in the competition should bring a laptop, and any tools that might reasonably be required for hacking embedded devices.

Links:

Website - <https://embeddedvillage.org/>

Game Hacking Village

Game Hacking Village: [Talk List](#)

Home Page: <https://gamehacking.gg/>

DC Village Page: https://defcon.org/html/defcon-34/dc-34-villages.html#orga_40967

Location: LVCCW Level 1 Hall 1 211 (Game Hacking Village) - [Map](#)

Social Media Links:

YT <https://youtube.com/@gamehackingvillage>

<https://x.com/GameHackingGG>

IG [@gamehacking.gg](#)

DC <https://discord.com/invite/bNYz8Xws8j>



A community dedicated to game security. Come play with hands-on reversing, modding, exploring, and exploiting games across various platforms. Our goal is to make game security accessible, learnable and playable for all skill levels. Game security is an exciting way to understand modern security concerns in a fun and interactive way.

Prerequisites

Some content may require a laptop. Certain talks and workshops may have some base knowledge required, but we also offer game hacking 101 material as well to get started with no prior knowledge.

Links:

Website - <https://gamehacking.gg>

[Return to Index](#)

Hardware Hacking and Soldering Skills Village (HHV-SSV)

Hardware Hacking and Soldering Skills Village (HHV-SSV): [Talk List](#)

Home Page: <https://dchhv.org/>

Sched Page: <https://dchhv.org/schedule/schedule.html>

DC Village Page: https://defcon.org/html/defcon-34/dc-34-villages.html#orga_40733

Location: LVCCW Level 1 Hall 1 400 (Hardware Hacking Village and Solder Skills Village) - [Map](#)

Social Media Links:

TW [@DC_HHV](#)

https://defcon.social/@DC_HHV



Every day our lives become more connected to consumer hardware. Every day the approved uses of that hardware are reduced, while the real capabilities expand. Come discover hardware hacking tricks and tips regain some of that capacity, and make your own use for things! We have interactive demos to help you learn new skills. We have challenges to compete against fellow attendees. We have some tools to help with your fever dream modifications. Come share what you know and learn something new.

Prerequisites:

Tools are all provided. Bringing your own setup if you have one will allow users to use a path they are familiar with.

Links:

Website - <https://dchhv.org>

Mastodon (@DC_HHV@defcon.social) - https://defcon.social/@DC_HHV

Website - <https://ddhhv.org>

[Return to Index](#)

Ham Radio Village

Ham Radio Village: [Talk List](#)

Home Page: <https://hamvillage.org/>

Sched Page: <https://cfp.hamvillage.org/dc34/talk/>

DC Village Page: https://defcon.org/html/defcon-34/dc-34-villages.html#orga_40732

Location: LVCCW Level 3 W315 (Ham Radio Village) - [Map](#)

Social Media Links:

TW [@HamRadioVillage](#)



The Ham Radio Village (HRV) is your home base for all things amateur radio; whether you've never touched a radio or you're already licensed and looking to branch out. From getting licensed and making your first transmission, to hacking and modifying radio/antenna hardware, to prowling on the hunt for radio 'foxes', there's something here for every level of curiosity. Attendees will walk away with hands-on radio frequency (RF) knowledge immediately applicable to other DEF CON contests, talks, and village demos. Interacting with licensed hams and other wireless enthusiasts will discover how ham radio knowledge transfers directly to RFID hacking, WiFi, and other wireless security work.

Have questions about ham radio? Come ask them. HRV is an open space for anyone curious about amateur radio; from first-timers to seasoned operators. Presented talks, contests, and volunteer tables cover everything from different modes of communication (voice, digital, Morse code) to the nuts and bolts of antenna design and signal propagation. Topics that typically carry a high barrier to entry become a lot more approachable when you can just walk up and ask someone.

When it's time to go home, participants take with them a foundation with applications well beyond the conference; including

- Understanding the base concepts of amateur radio, including how to use it as part of their day to day life, both for regular talking as well as building community
- Connect with like minded folks year round who have a vested interest in the hobby
- Find out how to Legally transmit with 1500w of power, more than what you use to heat your hot pocket!
- Learn how the radio hobby and radiosport can improve your hacking skills, because AX25 is quite easy to understand when building a basic network
- Provide for the future of the hobby, where you can learn, as well as teach others, enhancing the hacker community

Links:

Mastodon (@hamradiovillage@defcon.social) - <https://defcon.social/@hamradiovillage>

Website - <https://hamvillage.org/>

[Return to Index](#)

Hackers.town

Hackers.town: [Talk List](#)

Home Page: <https://masto.hackers.town/>

[Return to Index](#)

ICS Village

ICS Village: [Talk List](#)

Home Page: <https://www.icsvillage.com/>

Sched Page: <https://icsvillage.com/defcon-34>

DC Village Page: https://defcon.org/html/defcon-34/dc-34-villages.html#orga_40734

Location: LVCCW Level 1 Hall 2 502 (ICS Village) - [Map](#)

Social Media Links:

TW [@ICS_Village](#)

LI [@icsvillage](#)

YT [link](#)

TI [@ics_village](#)



ICS Village is a non-profit organization with the purpose of providing education and awareness of Industrial Control System security.

Interactive simulated ICS environments, such as Hack the Plan(e)t and Howdy Neighbor, provide safe yet realistic examples to preserve safe, secure, and reliable operations. We bring real components such as Programmable Logic Controllers (PLC), Human Machine Interfaces (HMI), Remote Telemetry Units (RTU), and actuators, to simulate a realistic environment throughout different industrial sectors. Visitors can connect their laptops to assess these ICS devices with common security scanners, network sniffers to sniff the industrial traffic, and more!

Prerequisites

Laptops, no other required hardware. ICS Fundamentals is recommended.

Links:

Website - <https://www.icsvillage.com>

[Return to Index](#)

IoT Village

IoT Village: [Talk List](#)

Home Page: <https://www.iotvillage.org/>

Sched Page: <https://www.iotvillage.org/events/defcon-34/index.html>

DC Village Page: https://defcon.org/html/defcon-34/dc-34-villages.html#orga_40735

Location: LVCCW Level 1 Hall 1 215 (IoT Village) - [Map](#)

Social Media Links:

TW [@iotvillage](#)

TW [@ISEsecurity](#)

TW [@Villageidiotlab](#)

<https://defcon.social/@IoTVillage/>

TI [@iotvillage](#)

YT <https://www.youtube.com/c/IoTVillage/videos>

DC <https://discord.gg/EFKbNFrFaN>



Hack all the things at IoT Village!

IoT Village advocates for advancing security in the Internet of Things (IoT) industry through bringing researchers and industry together. IoT Village hosts talks by expert security researchers, interactive hacking labs, live bug hunting in the latest IoT tech, and competitive IoT hacking contests. Over the years IoT Village has served as a platform to showcase and uncover hundreds of new vulnerabilities, giving attendees the opportunity to learn about the most innovative techniques to both hack and secure IoT. IoT Village is organized by security consulting and research firm, Independent Security Evaluators (ISE).

Prerequisites

IoT Village welcomes individuals of all skill levels. A base knowledge of HTML is a nice to have, but we offer activities for everyone. Bringing your own laptop could help in beating around long lines for terminals for hands-on labs.

Links:

Website - <https://iotvillage.org/>

[Return to Index](#)

Lonely Hackers Club

Lonely Hackers Club: [Talk List](#)

Home Page: <https://lonelyhackers.club/>

Social Media Links:

<https://lonelyhackers.club/telegram/>

<https://x.com/L0nelyH4ckers>

<https://defcon.social/@L0nelyH4ckers>

[Return to Index](#)

LockPick Village

LockPick Village: [Talk List](#)

Home Page: <https://www.toool.us/>

DC Village Page: https://defcon.org/html/defcon-34/dc-34-villages.html#orga_40736

Location: LVCCW Level 1 Hall 1 407 (Lockpick Village) - [Map](#)

Social Media Links:

TW [@toool](#)

TI [@toool_us](#)

YT <https://youtube.com/c/TOOOL-US>

<https://techhub.social/@TOOOL>

DC <https://discord.gg/KVzJ9QK2az>



Want to tinker with locks and tools the likes of which you've only seen in movies featuring secret agents, daring heists, or covert entry teams?

Then come on by the Lockpick Village, run by The Open Organization Of Lockpickers (TOOOL), where you will have the opportunity to learn hands-on how the fundamental hardware of physical security operates and how it can be compromised.

The Lockpick Village is a physical security demonstration and participation area. Visitors can learn about the vulnerabilities of various locking devices, techniques used to exploit these vulnerabilities, and practice on locks of various levels of difficulty to try it themselves.

Experts will be on hand to demonstrate and plenty of trial locks, pick tools, and other devices will be available for you to handle. By exploring the faults and flaws in many popular lock designs, you can not only learn about the fun hobby of sport-picking, but also gain a much stronger knowledge about the best methods and practices for protecting your own property.

Links:

Mastodon (@TOOOL@techhub.social) - <https://techhub.social/@TOOOL>

Website - <https://toool.us/>

[Return to Index](#)

La Villa Community

La Villa Community: [Talk List](#)

Home Page: <https://lavillahacker.com/>

Social Media Links:

<https://x.com/lavillahacker>

LI [@la-villa-hacker](#)

IG [@lavillahacker](#)

[Return to Index](#)

Middle Easterns & Africans in Cyber Security (MEACS)

Middle Easterns & Africans in Cyber Security (MEACS): [Talk List](#)

Home Page: <https://meacs.org/>

[Return to Index](#)

Mobile Hacking Community

Mobile Hacking Community: [Talk List](#)

Home Page: <https://mobilehackingcommunity.com/>

Sched Page: <https://mobilehackingcommunity.com/schedule/>

Social Media Links:

DC <https://discord.gg/dHW7PVSCzY>

<https://mastodon.social/@mobilehackingcommunity>

[Return to Index](#)

Maritime Hacking Village

Maritime Hacking Village: [Talk List](#)

Home Page: <https://maritimehackingvillage.com/>

Sched Page: <https://maritimehackingvillage.com/dc34>

DC Village Page: https://defcon.org/html/defcon-34/dc-34-villages.html#orga_40969

Location: LVCCW Level 1 Hall 2 703 (Maritime Hacking Village) - [Map](#)

Social Media Links:

<https://x.com/maritimevillage>

LI [@maritimehackingvillage](#)



The Maritime Hacking Village (MHV) has set sail for Las Vegas to deliver the next evolution of our immersive maritime hacking experience for the participants of DEF CON 34 to learn what it takes to exploit and defend real-world maritime systems. Our mission is simple: we are creating a space for hackers, stakeholders, and policy makers to come together and navigate the changing tides in the maritime sector's technological, geopolitical, and adversarial landscapes which demand ever-more-urgent collective action to address the systemic cybersecurity vulnerabilities in the systems which underpin global maritime defense and trade.

Maritime infrastructure is the undeniable backbone of our global economy and society as we know it. It is central to the supply chains for nearly all critical infrastructure -- and still, stakeholders unanimously agree that maritime systems (ships, ports, and maritime communication infrastructure) are some of the most digitally vulnerable, and that the sector has systemically under-invested in developing the policy, tools, and workforce necessary to change this. Evidently these are issues that require engagement with the security community to solve -- but seemingly insurmountable access barriers prevent the security community, and anyone else, from doing anything to help -- and so, as we see it, these access barriers have become the primary issue which stands in the way of progress.

MHV has made it our purpose to eliminate these barriers, and provide every human with the access and resources necessary to engage in maritime vulnerability research and cybersecurity innovation. Together we hack to facilitate the discovery and sharing of knowledge integral to the development of effective maritime cybersecurity policy, industry standards and regulations, vulnerability information sharing, cyber threat intelligence, and most importantly -- a capable and trusted workforce. Our village is a safe, shared space where the security community (elite hackers, trusted providers, and young talent alike) can develop and demonstrate their competence in attacking and defending real maritime systems -- and where maritime industry stakeholders can engage with this community to find trustworthy security professionals to help their cause, to

discover tools and techniques to protect their systems, and to access a talent pipeline to feed their next-generation workforce. We believe that this work together will create rising tides of awareness, information sharing, and innovation that will lift all ships and allow us to gradually secure the maritime sector.

Prerequisites

Ideally, participants will be familiar with using a terminal, the screen utility, basic /dev/tty devices, and wireshark. Beyond this, there are no hard prerequisites, but participating individuals and teams are encouraged to bring experience in the following areas to accelerate successful engagement in our more advanced hacking challenges:

- CAN-based protocols, ex. CAN bus, J1939, NMEA2000. Familiarity using can-utils
- Serial protocols, ex. Modbus (RS485 and tcp), NMEA0183 (RS422), and RS232
- SDR/software defined radio - basic usage of gnuradio with HackRF or more advanced radio
- Firmware/binary analysis and reverse engineering
- Attacking WiFi (802.11) networks
- Understanding of common radio frequency modulation schemes
- Familiarity with LoRA and 802-based mesh networking

Links:

Website - <https://maritimehackingvillage.com/>

Mastodon (@maritimehackingvillage@defcon.social) - <https://defcon.social/@maritimehackingvillage>

[Return to Index](#)

Misc

Misc: [Talk List](#)

[Return to Index](#)

Maker's Village

Maker's Village: [Talk List](#)

Home Page: <https://makersvillage.space/>

Sched Page: <https://makersvillage.space/#content16-23>

DC Village Page: https://defcon.org/html/defcon-34/dc-34-villages.html#orga_41289

Location: LVCCW Level 1 Hall 1 301 (Makers' Village) - [Map](#)

Social Media Links:

DC <https://discord.gg/VBwjCCvqG>



The Makers Village is an artistic, hands-on creative lab where DEF CON attendees can explore modern making as a form of hacking through design, experimentation, and fabrication. This space introduces participants to the tools and processes used in today's maker movement — including 3D printing, digital design software, textile machines, laser etchers and cutting tools, two-part epoxy and resin work, and other creative fabrication techniques. Attendees can expect to learn how ideas move from concept to physical object while experimenting with materials, machines, and workflows in a supportive environment.

Prerequisites

Makers of all experiences welcome. Learners under 18 need their responsible adult... or as responsible as DEF CON gets.

Links:

Website - <https://makersvillage.space>

[Return to Index](#)

Malware Village

Malware Village: [Talk List](#)

Home Page: <https://malwarevillage.org/>

DC Village Page: https://defcon.org/html/defcon-34/dc-34-villages.html#orga_40968

Location: LVCCW Level 1 Hall 2 600 (Malware Village) - [Map](#)

Social Media Links:

<https://x.com/MalwareVillage>

LI [@malwarevillage](#)

DC <https://discord.com/invite/xQwqY48SrJ>



Malware Village is dedicated to providing a safe and engaging environment for participants to learn and share knowledge about malware analysis. Our mission is to equip attendees with the skills, techniques, and historical context needed to understand, research, and combat malware. Participants will gain hands-on experience with real-world analysis techniques, guided by seasoned infosec professionals.

Village participants will have opportunities to immerse themselves in various aspects of malware-analysis under the guidance of (and supported by) experienced infosec professionals. Malware Village also provides participants opportunities to connect and network with infosec professionals and malware-analysis enthusiasts.

Beyond technical training, Malware Village fosters a strong community where researchers, enthusiasts, and professionals can connect. We welcome everyone—whether you're an artist creating malware-inspired art, a hardware researcher discovering unexpected connections to malware analysis, or a seasoned analyst reminiscing about early malware history.

Prerequisites

- ◊ For talks, there is no requirement just come and learn
- ◊ For workshops, an attendee will likely need the use of a laptop

Links:

Website - <https://malwarevillage.org>

Mastodon (@malwarevillage@defcon.social) - <https://defcon.social/@malwarevillage>

[Return to Index](#)

Nix Vegas Community

Nix Vegas Community: [Talk List](#)

Home Page: <https://nix.vegas/>

Social Media Links:

<https://x.com/NixVegas>

<https://bsky.app/profile/nixvegas.bsky.social>

<https://github.com/NixVegas>

YT <https://www.youtube.com/@NixVegasDEFCON>

<https://live.nix.vegas/>

[Return to Index](#)

Noob Community

Noob Community: [Talk List](#)

[Return to Index](#)

OSINT For Good Community

OSINT For Good Community: [Talk List](#)

Home Page: <https://www.tracelabs.org/>

Social Media Links:

<https://infosec.exchange/@tracelabs>

TW [@TraceLabs](#)

YT <https://www.youtube.com/c/TraceLabsVideos>

LI [@tracelabs](#)

<https://github.com/tracelabs>

[Return to Index](#)

OWASP Foundation

OWASP Foundation: [Talk List](#)

Home Page: <https://owasp.org/>

Social Media Links:

<https://infosec.exchange/@owasp>

YT <https://www.youtube.com/user/OWASPGLOBAL>

TW [@owasp](#)

FB [@OWASPFoundation](#)

LI [@owasp](#)

SL <https://owasp.org/slack/invite>

<https://github.com/OWASP/>

[Return to Index](#)

Payment Village

Payment Village: [Talk List](#)

Home Page: <https://www.paymentvillage.org/>

DC Village Page: https://defcon.org/html/defcon-34/dc-34-villages.html#orga_40738

Location: LVCCW Level 2 W204-205 (Payment Village) - [Map](#)

Social Media Links:

<https://x.com/paymentvillage>

TI [@paymentvillage](#)

YT <https://www.youtube.com/c/PaymentVillage>

<https://t.me/paymentvillage>

LI [@payment-village](#)

[link](#)



Come to the Payment Village to learn about payment technologies! Payments play a crucial role in our daily lives, yet many of us lack an understanding of how they work. Our mission is to educate and cultivate the next generation of payment security experts and to foster open discussions around payments. We want to raise the bar in payment security! We invite you to explore the history of payments and to learn how modern-day payments work.

The village is jam-packed with hands-on experiences and exciting challenges! Unsure of where to start? Register for one of our workshops to acquire new skills or attend a talk by one of our carefully chosen experts. Already a pro? Pick up a Payment Village credit card to take part in our contest! Looking for unique challenges? Take home all the money from our cash-grab machine or have a go at our scavenger hunt!

Links:

Website - <https://paymentvillage.org>

[Return to Index](#)

Packet Hacking Village

Packet Hacking Village: [Talk List](#)

Home Page: <https://www.wallofsheep.com/>

Sched Page: <https://www.phvillage.io/pages/dc34/>

DC Village Page: https://defcon.org/html/defcon-34/dc-34-villages.html#orga_40737

Location: LVCCW Level 3 W303-310 (Packet Hacking Village) - [Map](#)

Social Media Links:

<https://x.com/wallofsheep>

FB [@wallofsheep](#)

YT <https://youtube.com/wallofsheep>

TI [@wallofsheep](#)

PS <https://www.periscope.tv/wallofsheep>

<https://defcon.social/@wallofsheep>

IG [@wallofsheep](#)



The Packet Hacking Village at DEF CON provides a community learning experience for people of all skill levels, from absolute beginners to seasoned professionals. While DEF CON is made up of dozens of small community-of-interest villages, we are one of the largest and most well known. We host practical training, network forensics and analysis games, and the renowned Capture The Packet event, which has been a Black Badge contest over 10 times and draws world-class hackers from around the world. Our mission has always been simple: to teach people good internet safety practices, and to provide an atmosphere that encourages everyone to explore and learn.

We provide a welcoming environment for hackers of all skill levels and backgrounds to network, learn new things, and be active participants in DEF CON. Our famous “Wall of Sheep” provides a fun and interactive take on internet security and privacy, while our contests Packet Inspector, Packet Detective, and Capture The Packet serve as a zero-to-hero pathway for individuals to learn network security, packet analysis, and delve into advanced security topics. Every year we strive to bring something new and innovative to DEF CON, whether it’s never-seen-before talks or creative games to teach and test skills.

Depending on what talks, contests, and events participants select, they can expect to learn any/all of the following: Basic Internet security and privacy, network cable construction, honeypot setup and operation, regex, Linux training, packet interception and decoding, network analysis, sniffing, and forensics, reverse engineering, file forensics, system forensics, cryptography analysis, and more to be determined by the talks and workshops that we accept.

The Packet Hacking Village and Wall of Sheep have been a part of DEF CON since DEF CON 9, and we are proud to provide education and training to the hacker community at no cost.

Links:

Website - <https://www.wallofsheep.com>

Mastodon (@wallofsheep@defcon.social) - <https://defcon.social/@wallofsheep>

[Return to Index](#)

Policy @ DEF CON

Policy @ DEF CON: [Talk List](#)

Home Page: <https://defcon.org/policy/>

Sched Page: <https://bsky.app/profile/defconpolicy.bsky.social/post/3mqhrqudiv22b>

DC Village Page: https://defcon.org/html/defcon-34/dc-34-villages.html#orga_40740

Location: LVCCW Level 2 W210-211 (Policy Village) - [Map](#)

Social Media Links:

TW [@DEFCONPolicy](#)

[link](#)

<https://defcon.social/@defconpolicy>

[link](#)

LI [@policy-def-con](#)

YT <https://www.youtube.com/@policyatdefcon>



DEF CON welcomes policymakers and technology professionals to join Policy@DEF CON and participate with our community of knowledgeable experts. We need to work together.

Over the past 30 years the DEF CON community, has evolved and grown along with the cyber domain. We understand that creating a safer digital society requires collaboration between security and policy experts. DEF CON provides a space for representatives of all areas of security to come together to educate and engage each other.

Tech policy is being written as we speak and we believe including diverse expert voices will improve outcomes across the policy-technology spectrum by bridging the gap between technical and policy practitioners. Senior government officials, policy experts, nonprofit and the private sector, security researchers, hackers, academics and technologists from around the world all come together at Policy @ DEF CON.

Links:

Website - <https://defcon.org/policy/>

[Return to Index](#)

Physical Security Village

Physical Security Village: [Talk List](#)

Home Page: <https://www.physsec.org/>

DC Village Page: https://defcon.org/html/defcon-34/dc-34-villages.html#orga_40970

Location: LVCCW Level 1 Hall 2 601 (Physical Security Village) - [Map](#)

Social Media Links:

TW [@physsec](#)

TI [@bypassvillage](#)

LI [@physsec](#)

<https://defcon.social/@physsec>

DC <https://discord.gg/XmuEF62eun>

IG [@physsecvillage](#)



The Physical Security Village explores the world of hardware bypasses and techniques generally outside of the realm of cyber-security and lockpicking. Come learn some of these bypasses, how to fix them, and have the opportunity to try them out for yourself. We'll be covering the basics, like the under-the-door-tool and latch slipping attacks, as well as an in depth look at more complicated bypasses. Learn about elevator hacking, attacking alarm systems at the sensor and communication line, and cut-away and display models of common hardware to show how it works on the inside!

Links:

Website - <https://www.physsec.org>

Mastodon (@physsec@defcon.social) - <https://defcon.social/@physsec>

[Return to Index](#)

Queercon Community

Queercon Community: [Talk List](#)

Home Page: <https://queercon.org/>

Social Media Links:

<https://bsky.app/profile/queercon.org>

DC <https://queercon.org/discord>

[Return to Index](#)

Quantum Village

Quantum Village: [Talk List](#)

Home Page: <https://quantumvillage.org/>

DC Village Page: https://defcon.org/html/defcon-34/dc-34-villages.html#orga_40741

Location: LVCCW Level 1 Hall 2 605 (Quantum Village) - [Map](#)

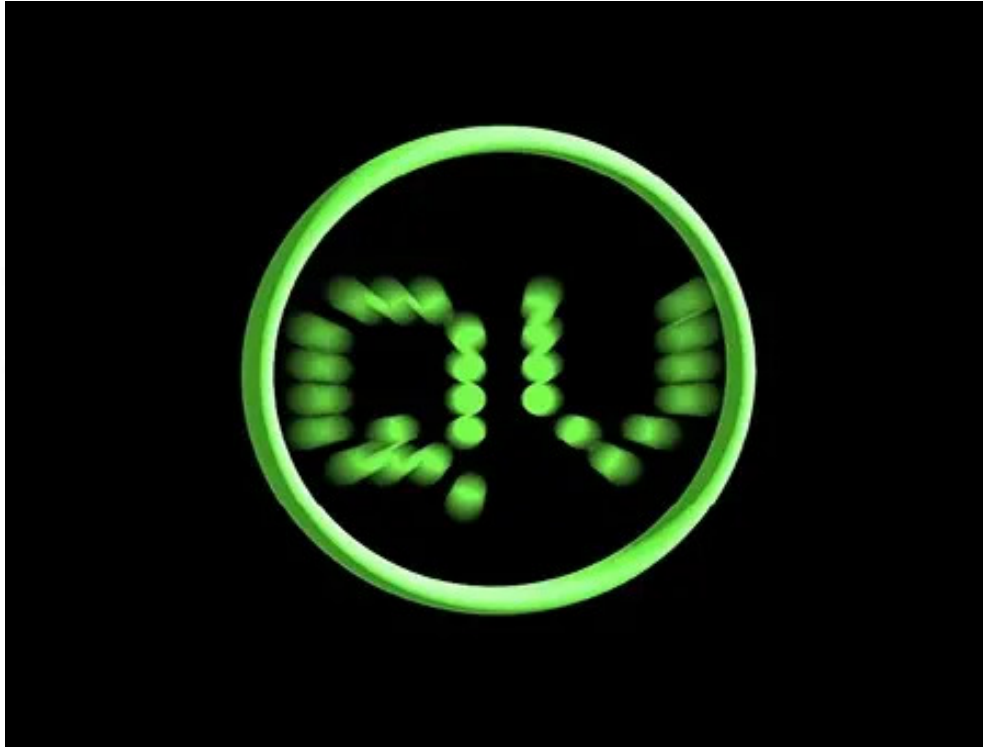
Social Media Links:

TW [@quantum_village](#)

DC <https://discord.gg/6WUjH5cBXu>

LI [@quantumvillage](#)

YT https://youtube.com/@quantum_village/



We are excited to bring you the 5th Edition of Quantum Village @ Def Con! Last year was a blast and our open source hardware sparked a revolution in quantum tech, and we have only just begun! QV provides vital resources and spaces for the hacker community to have access to quantum hardware and start designing the next generation of quantum technologies on their own terms.

This year we are bringing even more Open Quantum Hardware to Vegas, and we want you to come and be part of this seismic shift in how we innovate and adopt these exciting new technologies and ideas. You wanted more quantum, and quantum needs your Hacker Ingenuity!

With most of quantum tech being the preserve of academics and venture capitalists, we believe the Quantum Village is a vital space that hackers of all capabilities can benefit from and deserve. Let's build stuff from the Atom Up!

Links:

Website - <https://quantumvillage.org/>

[Return to Index](#)

Recon Village

Recon Village: [Talk List](#)

Home Page: <https://reconvillage.org/>

Sched Page: <https://reconvillage.org/reconvillage-2026-defcon-34/talks>

DC Village Page: https://defcon.org/html/defcon-34/dc-34-villages.html#orga_40743

Location: LVCCW Level 1 Hall 2 501 (Recon Village) - [Map](#)

Social Media Links:

<https://x.com/ReconVillage>

FB [@reconvillage](#)

YT <https://www.youtube.com/reconvillage/>

https://www.threads.com/@recon_villa

LI [@reconvillage](#)

DC <https://discord.gg/reconvillage>



Recon Village is an Open Space with Talks, Live Demos, Workshops, Discussions, Beginner Sessions, and CTFs, all centered around one theme: Reconnaissance.

Here, you explore recon and OSINT as practical disciplines across security research, investigation, journalism, and intelligence. You will learn how to map infrastructure, trace digital footprints, analyze open data, pivot across sources, and understand how systems, people, and signals connect across internet, cloud, AI, and the physical world.

Expect GeOSINT, live recon, do your own recon sessions, recon dashboards, and practitioner-led talks that go deep into real tradecraft.

You will not just listen. You will investigate, enumerate, validate, and think. If you want to see what is exposed before others do, and turn scattered signals into actionable insight, this is your space.

Prerequisites

Not a lot is needed to participate in Recon Village.

If you plan to participate seriously in contests such as CTFs, live recon, or GeOSINT challenges, a laptop is strongly recommended so you can enumerate, pivot, and document findings in real time. For lighter participation, a smartphone with internet access is sufficient.

There will be content and activities for all levels, from beginners exploring fundamentals to experienced practitioners diving into deeper investigations.

Good to Have - asic familiarity with domains, IP addresses, DNS, and search operators is helpful. Prior experience with command line tools or recon and OSINT frameworks is a plus, but not required.

Required mindset: curiosity, patience, and the instinct to follow the signal.

Links:

Website - <https://reconvillage.org>

Mastodon (@reconvillage@defcon.social) - <https://defcon.social/@reconvillage>

[Return to Index](#)

Radio Frequency Village

Radio Frequency Village: [Talk List](#)

Home Page: <https://rfhackers.com/>

DC Village Page: https://defcon.org/html/defcon-34/dc-34-villages.html#orga_40742

Location: LVCCW Level 1 Hall 1 409 (Radio Frequency Village) - [Map](#)

Social Media Links:

TW [@rfhackers](#)

TW [@rf_ctf](#)

[link](#)

DC <https://discordapp.com/invite/JjPQhKy>



After 20 years of evolution, from the WiFi Village, to the Wireless Village, RF Hackers Sanctuary presents: The Radio Frequency Village at DEF CON 34. The Radio Frequency Village is an environment where people come to learn about the

security of radio frequency (RF) transmissions, which includes wireless technology, applications of software defined radio (SDR), Bluetooth (BT), Zigbee, WiFi, Z-wave, Radio Frequency Identification (RFID), Infrared (IR) and other protocols within the usable RF spectrum. As a security community we have grown beyond WiFi, and even beyond Bluetooth and Zigbee. The RF Village includes talks on all manner of radio frequency command and control as well as communication systems. While everyone knows about the WiFi and Bluetooth attack surfaces, most of us rely on many additional technologies every day. RF Hackers Sanctuary is supported by a group of experts in the area of information security as it relates to RF technologies. RF Hackers Sanctuary's common purpose is to provide an environment in which participants may explore these technologies with a focus on improving their skills through offense and defense. These learning environments are provided in the form of guest speakers, panels, and Radio Frequency Capture the Flag games, to promote learning on cutting edge topics as it relates to radio communications. We promise to still provide free WiFi.

Co-located with the RF Village is the RF Capture the Flag. Come for the talks, stay for the practice and the competition.

Links:

Website - <http://rfhackers.com>

Website - <https://rfhackers.com>

[Return to Index](#)

Red Team Village

Red Team Village: [Talk List](#)

Home Page: <https://redteamvillage.io/>

Sched Page: <https://redteamvillage.io/schedule>

DC Village Page: https://defcon.org/html/defcon-34/dc-34-villages.html#orga_40744

Location: LVCCW Level 1 Hall 1 309 (Red Team Village) - [Map](#)

Social Media Links:

https://x.com/redteamvillage_

YT <https://www.youtube.com/redteamvillage>

TI [@redteamvillage](#)

DC <https://discord.gg/redteamvillage>

IG [@theredteamvillage](#)

[link](#)



The Red Team Village is focused on training the art of critical thinking, collaboration, and strategy in offensive security. The RTV brings together information security professionals to share new tactics and techniques in offensive security. Attendees may spend time engaged in workshops or challenge themselves in an immersive Capture the Flag competition to put their newly obtained skills to the test.

Prerequisites

Laptops are highly encouraged for participation in Red Team Village tactics and workshops, and are mandatory for CTF and Wargames.

Links:

Website - <https://redteamvillage.io/>

[Return to Index](#)

Scambait Village

Scambait Village: [Talk List](#)

Home Page: <https://teamtda.org/>

DC Village Page: https://defcon.org/html/defcon-34/dc-34-villages.html#orga_41428

Location: LVCCW Level 1 Hall 1 208 (Scambait Village) - [Map](#)



Learn the art of Scambaiting. Speak with experts in our community to get an introduction to the skills needed to better understand common scams & fraud. Explore ethical OSINT used to track criminal infrastructure and learn the Social Engineering tactics required for disrupting call center operations. We'll cover the foundations of identifying victims, reporting to authorities, and safely navigating the world of counter-fraud. Stop hanging up and start learning how to hit back.

Prerequisites

◇ Laptop or phone with internet connection to join sessions with live scam bait calls to listen or join in.

[Return to Index](#)

Social Engineering Community Village

Social Engineering Community Village: [Talk List](#)

Home Page: <https://www.se.community/>

Sched Page: <https://se.community/schedule/>

DC Village Page: https://defcon.org/html/defcon-34/dc-34-villages.html#orga_40745

Location: LVCCW Level 3 W317-319 (Social Engineering Community Village) - [Map](#)

Social Media Links:

TW [@sec_defcon](#)

YT [link](#)

TI [@se_community](#)

LI [@social-engineering-community](#)

FB [@Social-Engineering-Community-108883855139272](#)



The Social Engineering Community village dives into one of the most powerful attack surfaces in security: humans. Our village creates a space where attendees can explore the psychology, tactics, and tradecraft behind human-focused hacking. Through presentations, live demonstrations (via contests), and interactive activities, students, defenders, hackers, and the curious can see how reconnaissance, persuasion, and improvisation are used to bypass even the best defenses.

At DEF CON the village becomes a live stage for the craft. In the Social Engineering Community Vishing Competition (SECVC), competitors step into a soundproof booth and place real calls using OSINT, creative pretexts, and quick thinking while the audience watches the strategy unfold in real time. In Battle of the Bots, human-created AI agents attempt social engineering calls of their own, exploring what happens when automated systems try their hand at elicitation. Alongside the contests, attendees can have the opportunity to place calls in our "Cold Calls" or listen in to some presentations.

The village is built by the community that practices the craft. Volunteers, researchers, hackers, defenders, and curious newcomers all contribute to the content each year, creating space for new voices and ideas to take the stage. Whether you want to watch live un-scripted social engineering calls, understand the psychology behind it, or meet others who love the human side of security, the Social Engineering Community village is the place to experience it at DEF CON.

Prerequisites

Attendees are welcome to watch contests, join discussions, and participate in interactive activities with no preparation needed.

Competitors in the Social Engineering Community Vishing Competition and Battle of the Bots Contest are selected in advance through a Call for Competitors prior to DEF CON, but some activities such as Cold Calls allow audience members to sign up onsite and participate.

Attendees who want to participate in Cold Calls may benefit from brushing up on basic social engineering skills such as rapport building, influence and elicitation techniques.

Links:

Website - <https://www.se.community>

Website - <https://www.se.community/>

[Return to Index](#)

Social Gatherings/Events

Social Gatherings/Events: [Talk List](#)

Home Page: <https://defcon.outel.org/dcwp/dc34/activities/pge/>

[Return to Index](#)

The Diana Initiative

The Diana Initiative: [Talk List](#)

Home Page: <https://www.dianainitiative.org/home>

Social Media Links:

<https://defcon.social/@DianaInitiative>

FB [@dianainitiative](#)

<https://x.com/DianaInitiative>

[link](#)

YT [link](#)

IG [@dianainitiative](#)

[Return to Index](#)

Telecom Village

Telecom Village: [Talk List](#)

Home Page: <https://telecomvillage.com/>

DC Village Page: https://defcon.org/html/defcon-34/dc-34-villages.html#orga_40747

Location: LVCCW Level 3 W321 (Telecom Village) - [Map](#)

Social Media Links:

<https://x.com/TelecomVillage>

LI [@telecom-village](#)



The Telecom Security Village focuses on the intersection of telecommunications infrastructure, security operations, and advanced threat research. As telecom networks form the backbone of global communication, they have become a high-value target for Advanced Persistent Threats (APTs), nation-state actors, and sophisticated cybercriminal groups. This village explores how modern telecom environments—including 4G/5G core networks, signaling systems, IMS infrastructure, and routing protocols such as BGP—are monitored, defended, and analyzed within a telecom Security Operations Center (SOC).

Attendees will learn how telecom SOC teams detect and investigate threats targeting mobile networks, signaling systems, and subscriber infrastructure. The village will demonstrate techniques used to identify signaling abuse, network manipulation, SIM and identity attacks, and telecom-specific intrusion patterns that are often leveraged by APT groups for surveillance, interception, and disruption.

Through talks, live demonstrations, and research discussions, participants will gain insight into telecom threat intelligence, network telemetry analysis, anomaly detection in signaling networks, and defensive strategies used by operators and researchers to protect critical communications infrastructure. The goal of the Telecom Security Village is to bridge the gap between the telecom engineering community and the cybersecurity research ecosystem while promoting deeper understanding of threats targeting global telecom networks.

Prerequisites

Participants do not need prior telecom experience to attend the Telecom Security Village, but a basic understanding of networking concepts will be helpful. Familiarity with IP networking, TCP/IP protocols, and general cybersecurity concepts will allow attendees to gain more value from the hands-on demonstrations and discussions.

For technical workshops and labs, participants are encouraged to have some exposure to Linux environments, packet analysis tools such as Wireshark, and basic scripting or programming knowledge (e.g., Python). Attendees interested in deeper exploration may benefit from familiarity with mobile network concepts such as LTE/5G architecture, SIP/IMS signaling, or routing protocols like BGP, though these are not strict requirements.

The village is designed to accommodate a broad audience including security researchers, telecom engineers, network operators, students, and hackers who are interested in understanding telecom infrastructure and its security challenges. Introductory explanations will be provided so that newcomers can follow along while more advanced participants can engage with deeper technical content.

Links:

Mastodon (@akibsayyed@mastodon.social) - <https://mastodon.social/@akibsayyed>

Website - <https://telecomvillage.com>

[Return to Index](#)

Tamper Evident Village

Tamper Evident Village: [Talk List](#)

DC Village Page: https://defcon.org/html/defcon-34/dc-34-villages.html#orga_41508

Location: LVCCW Level 1 Hall 1 406 (Tamper Evident) - [Map](#)

"Tamper-evident" refers to a physical security technology that provides evidence of tampering (access, damage, repair, or replacement) to determine authenticity or integrity of a container or object(s). In practical terms, this can be a piece of tape that closes an envelope, a plastic detainer that secures a hasp, or an ink used to identify a legitimate document. Tamper-evident technologies are often confused with "tamper resistant" or "tamper proof" technologies which attempt to prevent tampering in the first place. Referred to individually as ""seals,"" many tamper technologies are easy to destroy, but a destroyed (or missing) seal would provide evidence of tampering! The goal of the TEV is to teach attendees how these technologies work and how many can be tampered with without leaving evidence.

The Tamper-Evident Village includes the following contests and events:

- ****The Box (Bomb Defusal Contest)**** - The Box is an electronic tamper-evident challenge in which you have 10 minutes to defuse a bomb. Learn about electronic sensors, traps, and other crafty tricks while solving puzzles to figure out how to defuse the bomb. One mistake lets The Box know you're doing something you shouldn't and BOOM, you're dead. Make every second count! Don't worry - you can respawn at the back of the line.
 - **** Tamper-Evident Contest: King of the Hill**** - Compete against your fellow DEF CON attendees identifying and exploiting tamper-evident seal defeats! Work with several mechanical tamper seals to figure out how they can be defeated and fool the would-be seal inspectors. Score is based on how hard it is for inspectors to identify tampering and how much time it took. Beat the current best and claim your spot as King of the Hill!
 - ****Counterfeit Badge Contest**** - Submit your best forgery of a DEF CON human badge. Other (non DEF CON) target badges are also available for those looking for more counterfeit challenges and fun! Please play responsibly and do not use counterfeit badges for untoward purposes at con.
-

[Return to Index](#)

DEF CON Training

DEF CON Training: [Talk List](#)

Home Page: <https://training.defcon.org/collections/def-con-training-las-vegas-2026>

DC Forums Page: <https://forum.defcon.org/node/244768>

[Return to Index](#)

Voting Village

Voting Village: [Talk List](#)

Home Page: <https://votingvillage.org/>

DC Village Page: https://defcon.org/html/defcon-34/dc-34-villages.html#orga_40748

Location: LVCCW Level 2 W219-220 (Voting Village) - [Map](#)

Social Media Links:

<https://x.com/votingvillagedc>

YT <https://youtube.com/@defconvotingvillage>

TI [@votingvillagedc](#)

LI [@election-integrity-foundation](#)

IG [@votingvillage?igsh=MWJreTh6dGl3eDEzNg==](#)



Voting Village at DEF CON, launched in 2017, is the first public forum where hackers and members of the public have legal, unconstrained, hands-on experience with actual election systems used in the United States and elsewhere. It has become the premier venue for exploring the theory and practice of election security. This unique voting laboratory helps participants – in person and around the world – understand where gaps in security are, how to mitigate vulnerabilities, and why hackers are such an important part of investigating election security. Most importantly, the Voting Village helps election officials at all levels understand how to make systems more secure and more trustworthy.

The Voting Village returns for its 10th year at DEF CON 34. As in the past, the Voting Village will feature a 2-day speaking track (Friday and Saturday) that will highlight various aspects of election cybersecurity, including the technical components that make up our election infrastructure: hardware, software, and databases, new vulnerabilities, and ways to mitigate them.

[Return to Index](#)

Talk/Event Schedule

Thursday

This Schedule is tentative and may be changed at any time. Check [here](#), [Hacker Tracker](#), or the nearest NFO Node for the latest.

Thursday - 06:00 PDT

[Return to Index](#) - [Locations Legend](#)

[Social Gatherings/Events](#) - [Defcon.run](#) -

[Return to Index](#) - [Locations Legend](#)

[Social Gatherings/Events](#) - [Human Registration Open](#) -

[Social Gatherings/Events](#) - [Merch \(formerly swag\) Area Open -- README](#) -

[Return to Index](#) - [Locations Legend](#)

[Social Gatherings/Events](#) - cont...(08:00-18:59 PDT) - [Human Registration Open](#) -
[Social Gatherings/Events](#) - cont...(08:00-17:59 PDT) - [Merch \(formerly swag\) Area Open -- README](#) -

Thursday - 10:00 PDT

[Return to Index](#) - [Locations Legend](#)

[DEF CON Groups](#) - [DEF CON Groups \(DCG\)](#) -

[Social Gatherings/Events](#) - [cont...\(08:00-18:59 PDT\)](#) - [Human Registration Open](#) -

[Social Gatherings/Events](#) - [cont...\(08:00-17:59 PDT\)](#) - [Merch \(formerly swag\) Area Open -- README](#) -

[Social Gatherings/Events](#) - [Music](#) - [SomaFM](#) -

[Social Gatherings/Events](#) - [Ham In A Day Class](#) -

Thursday - 11:00 PDT

[Return to Index](#) - [Locations Legend](#)

[DEF CON Groups](#) - cont...(10:00-17:59 PDT) - [DEF CON Groups \(DCG\)](#) -
[Social Gatherings/Events](#) - cont...(08:00-18:59 PDT) - [Human Registration Open](#) -
[Social Gatherings/Events](#) - cont...(08:00-17:59 PDT) - [Merch \(formerly swag\) Area Open -- README](#) -
[Social Gatherings/Events](#) - cont...(10:00-18:59 PDT) - [Music - SomaFM](#) -
[Social Gatherings/Events](#) - cont...(10:00-16:59 PDT) - [Ham In A Day Class](#) -

Thursday - 12:00 PDT

[Return to Index](#) - [Locations Legend](#)

[DEF CON Groups](#) - cont...(10:00-17:59 PDT) - [DEF CON Groups \(DCG\)](#) -
[Social Gatherings/Events](#) - cont...(08:00-18:59 PDT) - [Human Registration Open](#) -
[Social Gatherings/Events](#) - cont...(08:00-17:59 PDT) - [Merch \(formerly swag\) Area Open -- README](#) -
[Social Gatherings/Events](#) - cont...(10:00-18:59 PDT) - [Music](#) - [SomaFM](#) -
[Social Gatherings/Events](#) - [Friends of Bill W](#) -
[Social Gatherings/Events](#) - cont...(10:00-16:59 PDT) - [Ham In A Day Class](#) -

Thursday - 13:00 PDT

[Return to Index](#) - [Locations Legend](#)

[DEF CON Groups](#) - cont...(10:00-17:59 PDT) - [DEF CON Groups \(DCG\)](#) -
[Social Gatherings/Events](#) - cont...(08:00-18:59 PDT) - [Human Registration Open](#) -
[Social Gatherings/Events](#) - cont...(08:00-17:59 PDT) - [Merch \(formerly swag\) Area Open -- README](#) -
[Social Gatherings/Events](#) - cont...(10:00-18:59 PDT) - [Music - SomaFM](#) -
[Social Gatherings/Events](#) - cont...(10:00-16:59 PDT) - [Ham In A Day Class](#) -

Thursday - 14:00 PDT

[Return to Index](#) - [Locations Legend](#)

[DEF CON Groups](#) - cont...(10:00-17:59 PDT) - [DEF CON Groups \(DCG\)](#) -
[Social Gatherings/Events](#) - cont...(08:00-18:59 PDT) - [Human Registration Open](#) -
[Social Gatherings/Events](#) - cont...(08:00-17:59 PDT) - [Merch \(formerly swag\) Area Open -- README](#) -
[Social Gatherings/Events](#) - cont...(10:00-18:59 PDT) - [Music - SomaFM](#) -
[Social Gatherings/Events](#) - cont...(10:00-16:59 PDT) - [Ham In A Day Class](#) -

Thursday - 15:00 PDT

[Return to Index](#) - [Locations Legend](#)

[DEF CON Groups](#) - cont...(10:00-17:59 PDT) - [DEF CON Groups \(DCG\)](#) -
[Social Gatherings/Events](#) - cont...(08:00-18:59 PDT) - [Human Registration Open](#) -
[Social Gatherings/Events](#) - cont...(08:00-17:59 PDT) - [Merch \(formerly swag\) Area Open -- README](#) -
[Social Gatherings/Events](#) - cont...(10:00-18:59 PDT) - [Music - SomaFM](#) -
[Social Gatherings/Events](#) - cont...(10:00-16:59 PDT) - [Ham In A Day Class](#) -
[Social Gatherings/Events](#) - [Toxic BBQ](#) -

Thursday - 16:00 PDT

[Return to Index](#) - [Locations Legend](#)

[Data Duplication Village](#) - [DDV open and accepting drives for duplication](#) -
[DEF CON Groups](#) - [cont...\(10:00-17:59 PDT\)](#) - [DEF CON Groups \(DCG\)](#) -
[Social Gatherings/Events](#) - [cont...\(08:00-18:59 PDT\)](#) - [Human Registration Open](#) -
[Social Gatherings/Events](#) - [cont...\(08:00-17:59 PDT\)](#) - [Merch \(formerly swag\) Area Open -- README](#) -
[Social Gatherings/Events](#) - [cont...\(10:00-18:59 PDT\)](#) - [Music - SomaFM](#) -
[Social Gatherings/Events](#) - [cont...\(10:00-16:59 PDT\)](#) - [Ham In A Day Class](#) -
[Social Gatherings/Events](#) - [cont...\(15:00-20:59 PDT\)](#) - [Toxic BBQ](#) -

Thursday - 17:00 PDT

[Return to Index](#) - [Locations Legend](#)

[Data Duplication Village](#) - cont...(16:00-18:59 PDT) - [DDV open and accepting drives for duplication](#) -
[DEF CON Groups](#) - cont...(10:00-17:59 PDT) - [DEF CON Groups \(DCG\)](#) -
[Social Gatherings/Events](#) - cont...(08:00-18:59 PDT) - [Human Registration Open](#) -
[Social Gatherings/Events](#) - cont...(08:00-17:59 PDT) - [Merch \(formerly swag\) Area Open -- README](#) -
[Social Gatherings/Events](#) - cont...(10:00-18:59 PDT) - [Music - SomaFM](#) -
[Social Gatherings/Events](#) - [Friends of Bill W](#) -
[Social Gatherings/Events](#) - cont...(15:00-20:59 PDT) - [Toxic BBQ](#) -

Thursday - 18:00 PDT

[Return to Index](#) - [Locations Legend](#)

[Data Duplication Village](#) - cont...(16:00-18:59 PDT) - [DDV open and accepting drives for duplication](#) -

[Social Gatherings/Events](#) - cont...(08:00-18:59 PDT) - [Human Registration Open](#) -

[Social Gatherings/Events](#) - cont...(10:00-18:59 PDT) - [Music - SomaFM](#) -

[Social Gatherings/Events](#) - [Operator, Please Hold](#) - [DCG Social](#) -

[Social Gatherings/Events](#) - [Exploit Your Own Story](#) - Charel "1C0nur3r" Morris

[Social Gatherings/Events](#) - cont...(15:00-20:59 PDT) - [Toxic BBQ](#) -

[Social Gatherings/Events](#) - (18:30-23:30 PDT) - [Welcome Party at The Industrial](#) -

Thursday - 19:00 PDT

[Return to Index](#) - [Locations Legend](#)

[Social Gatherings/Events](#) - [Music](#) - [Genre: House](#) - [mattrix](#)

[Social Gatherings/Events](#) - [cont...\(18:00-19:59 PDT\)](#) - [Operator, Please Hold](#) - [DCG Social](#) -

[Social Gatherings/Events](#) - [cont...\(18:00-19:59 PDT\)](#) - [Exploit Your Own Story](#) - [Charel "1C0nur3r" Morris](#)

[Social Gatherings/Events](#) - [DC702 Meetup](#) -

[Social Gatherings/Events](#) - [cont...\(15:00-20:59 PDT\)](#) - [Toxic BBQ](#) -

[Social Gatherings/Events](#) - [cont...\(18:30-23:30 PDT\)](#) - [Welcome Party at The Industrial](#) -

Thursday - 20:00 PDT

[Return to Index](#) - [Locations Legend](#)

[Social Gatherings/Events](#) - [Music - Genre: Electro House](#) - [Archwisp](#)

[Social Gatherings/Events](#) - cont...(19:00-21:59 PDT) - [DC702 Meetup](#) -

[Social Gatherings/Events](#) - cont...(15:00-20:59 PDT) - [Toxic BBQ](#) -

[Social Gatherings/Events](#) - cont...(18:30-23:30 PDT) - [Welcome Party at The Industrial](#) -

Thursday - 21:00 PDT

[Return to Index](#) - [Locations Legend](#)

[Social Gatherings/Events](#) - [Music - Genre: Breakbeats](#) - [PatAttack](#)

[Social Gatherings/Events](#) - [Conference Planners Meetup](#) -

[Social Gatherings/Events](#) - cont...(19:00-21:59 PDT) - [DC702 Meetup](#) -

[Social Gatherings/Events](#) - cont...(18:30-23:30 PDT) - [Welcome Party at The Industrial](#) -

[Return to Index](#) - [Locations Legend](#)

[Social Gatherings/Events](#) - [Music](#) - [Genre: Breakbeats](#) - [Icetre Normal](#)

[Social Gatherings/Events](#) - cont...(21:00-23:59 PDT) - [Conference Planners Meetup](#) -

[Social Gatherings/Events](#) - cont...(18:30-23:30 PDT) - [Welcome Party at The Industrial](#) -

[Return to Index](#) - [Locations Legend](#)

[Social Gatherings/Events](#) - [Music](#) - [Genre: Techno](#) - [Scotch and Bubbles](#)
[Social Gatherings/Events](#) - cont...(21:00-23:59 PDT) - [Conference Planners Meetup](#) -
[Social Gatherings/Events](#) - cont...(18:30-23:30 PDT) - [Welcome Party at The Industrial](#) -

Friday

This Schedule is tentative and may be changed at any time. Check [here](#), [Hacker Tracker](#), or the nearest NFO Node for the latest.

Friday - 00:00 PDT

[Return to Index](#) - [Locations Legend](#)

[Social Gatherings/Events](#) - [Music](#) - [Genre: Techno](#) - [dotornot](#)

[Return to Index](#) - [Locations Legend](#)

[Social Gatherings/Events](#) - [Defcon.run](#) -

[Social Gatherings/Events](#) - [15th Cycleoverride Bike Ride at DEF CON](#) -

Friday - 07:00 PDT

[Return to Index](#) - [Locations Legend](#)

[Social Gatherings/Events](#) - cont...(06:00-07:59 PDT) - [Defcon.run](#) -

[Social Gatherings/Events](#) - cont...(06:00-10:59 PDT) - [15th Cycleoverride Bike Ride at DEF CON](#) -

Friday - 08:00 PDT

[Return to Index](#) - [Locations Legend](#)

[DEF CON Training](#) - (08:30-17:30 PDT) - [Beat the Breach: Defend, Respond, Survive](#) - McKay Hardy, Wes Wagstaff

[DEF CON Training](#) - (08:30-17:30 PDT) - [Cyber & AI Policy Basics: What Every Organization Needs in Place](#) - Pamela 'Pam' Feld, Greg Goldberg

[DEF CON Training](#) - (08:30-17:30 PDT) - [Digital Supply Chain Security: Software, Cryptography, AI, and Vendor Risk](#) - Anant Shrivastava, Sunil Yadav

[Social Engineering Community Village](#) - (08:30-17:59 PDT) - [Social Engineering Community Village](#) - Open Hours -

[Social Engineering Community Village](#) - (08:45-08:59 PDT) - [Village Greeting](#) -

[Social Gatherings/Events](#) - [Human Registration Open](#) -

[Social Gatherings/Events](#) - [Merch \(formerly swag\) Area Open -- README](#) -

[Social Gatherings/Events](#) - cont...(06:00-10:59 PDT) - [15th Cycleoverride Bike Ride at DEF CON](#) -

[Return to Index](#) - [Locations Legend](#)

[Contests](#) - [SEC Vishing Competition \(SEVCV\)](#) -

[DEF CON Training](#) - cont...(08:30-17:30 PDT) - [Beat the Breach: Defend, Respond, Survive](#) - McKay Hardy, Wes Wagstaff

[DEF CON Training](#) - cont...(08:30-17:30 PDT) - [Cyber & AI Policy Basics: What Every Organization Needs in Place](#) -

Pamela 'Pam' Feld, Greg Goldberg

[DEF CON Training](#) - cont...(08:30-17:30 PDT) - [Digital Supply Chain Security: Software, Cryptography, AI, and Vendor](#)

[Risk](#) - Anant Shrivastava, Sunil Yadav

[DEF CON Workshops](#) - [Sold Out](#) - [Offensive Packet Wizardry with Scapy](#) - Mike "Chicolinux" Guirao

[DEF CON Workshops](#) - [Sold Out](#) - [Hands-on IoT firmware extraction and flash forensics](#) - Dennis Giese, Braelynn

Luedtke, Arnold Wey, Harsha Potu

[DEF CON Workshops](#) - [Sold Out](#) - [AWS Cloud Security 101: From IAM Misconfigurations to Account Takeover](#) - zeta, Rafa

"bane" Gutierrez

[DEF CON Workshops](#) - [Sold Out](#) - [Web Hacking 101](#) - cale "calebot" smith, Ruchik Dave, Young Seuk Kim, Luke Cycon

[DEF CON Workshops](#) - [Sold Out](#) - [Malware Development 101](#) - [From Zero to Hero: Adapt your payload to your environment](#)

- Yoann "OtterHacker" DEQUEKER

[DEF CON Workshops](#) - [Sold Out](#) - [Long Live Empire: A C2 Workshop for Modern Red Teaming](#) - Jake "Hubbl3"

Krasnov, Vincent "Vinnybod" Rose, Anthony "Coin" Rose, Dan Niefeld

[DEF CON Workshops](#) - [Sold Out](#) - [Learning to Hack Bluetooth Low Energy with BLE CTF](#) - Ryan "Hackgnar"

Holeman, Alek Amrani

[DEF CON Workshops](#) - [Sold Out](#) - [Agentic Threat Hunting: Building AI That Remembers What You Hunted](#) - Sydney

"letswastetime" Marrone

[Social Engineering Community Village](#) - cont...(08:30-17:59 PDT) - [Social Engineering Community Village](#) - [Open Hours](#) -

[Social Gatherings/Events](#) - cont...(08:00-18:59 PDT) - [Human Registration Open](#) -

[Social Gatherings/Events](#) - cont...(08:00-17:59 PDT) - [Merch \(formerly swag\) Area Open -- README](#) -

[Social Gatherings/Events](#) - cont...(06:00-10:59 PDT) - [15th Cycleoverride Bike Ride at DEF CON](#) -

[Return to Index](#) - [Locations Legend](#)

[Aerospace Village - Aviation ISAC Cybersecurity Challenge](#) -
[Aerospace Village - Aerospace Ecosystem Resilience Innovation Environment \(AERIE\) Cyber Range](#) -
[Aerospace Village - ARINC 664 CTF Challenge](#) -
[Aerospace Village - DCNextGen - Bricks in the Air](#) -
[Aerospace Village - Drone Hacking Choose your Own Adventure](#) -
[Aerospace Village - DCNextGen - Space Grand Challenge - SatHack: The MOUSE-1 Mission](#) -
[Aerospace Village - DCNextGen - RIC-1: ELT Localization Exercise - N3VR-G0N Down](#) -
[Aerospace Village - Bricks in the Air](#) -
[Aerospace Village - Mission: Compromised - Hacking a Satellite from the Ground Up](#) -
[Aerospace Village - MOUSE Runner & Flappy Drone](#) -
[Aerospace Village - Flight Simulator/EFB](#) -
[Aerospace Village - Drone Hacking Workshop](#) -
[Aerospace Village - Satellites Under Attack: Hands-On Satellite Security Threat Scenarios](#) -
[Aerospace Village - Nebula Showdown: Space Systems Security CTF Adventure](#) -
[Aerospace Village - SR-71 Blackbird Badge Challenge](#) -
[Aerospace Village - SpaceCOP - Catch Me If You Can](#) -
[Aerospace Village - Hacking Electronic Conspicuity Devices -or- Making Light Aircraft Fly Into Conflict](#) - Ken Munroe
[AI Village - AI Village: Village Open](#) -
[AI Village - AI Village: Opening Remarks](#) -
[AI Village - Poster Presentations](#) -
[AI Village - Cyber Mirage: Realtime Deepfake Demos](#) - Brandon Kovacs
[AppSec Village - \(10:15-11:15 PDT\) - Pentesting made easy - Keeping sessions alive with session chains](#) - Kai Glauber,Matthias Göhring
[AppSec Village - \(10:30-12:30 PDT\) - Burp, But Yours: Hands-On Extension and Bambda Development](#) - Hannah L
[AppSec Village - \(10:30-10:59 PDT\) - The Dots Do Matter: Gmail's Invisible Blindspot](#) - Keren Elazari
[Biohacking Village - Biohacking Device Lab](#) -
[Biohacking Village - Embedded & Shredded: Advanced Embedded System Hacking](#) -
[Biohacking Village - Four Newbies Vs. An Insulin Pump. How Hard Can It Be?](#) - Birgitte Jordal,Julia Kucharska,Emilie Jørstad,Selma Jenker
[Biohacking Village - Counting the Dead in the Digital Siege: Detection Infrastructure for Cyber-Mapping Patient Harm](#) - Jorge Acevedo Canabal,Scott Shackelford,Szymon Skalski
[Blacks In Cyber Village - Return of the Defender: Using AI to Strike Back Against Enterprise Threats](#) - Levone Campbell
[Blue Team Village - Incident Response 101: Preparing Before the Hack, Responding After It](#) - Joshua Morgan
[Bug Bounty Village - The Future of Bug Bounty - Program Manager Perspective](#) - Jai Kumar Sharma,Catherine Cassell,Austin Sturm,Dane Sherrets,Sachin "sachinnthakuri" Thakuri
[Bug Bounty Village - Click Me: Turning URI Links into Bug Bounty RCE's](#) - Tobias Diehl
[Bug Bounty Village - \(10:30-11:30 PDT\) - Hacking IDE Extensions - VSCode Workshop](#) - Nick "7urb01" Copi
[Call Center Village - Call Center Village - Open](#) -
[Car Hacking Village - Bomb Bot Challenge](#) -
[Car Hacking Village - Car Hacking Village Open](#) -
[Cloud Village - Opening Talk](#) - Jayesh Singh Chauhan
[Cloud Village - New AWS IAM Attack Paths and the Framework to Exploit Them](#) - Seth Art
[Cloud Village - \(10:50-11:30 PDT\) - Tokens and PRT: Advanced Attacks and Persistence in Microsoft Entra ID](#) - Elzer Pineda,Jose Rivas
[CodeBloom - Game Time: Loops](#) -
[Contests - Aw, man...pages!](#) -
[Contests - 5N4CK3Y](#) -
[Contests - DC's Next Top Threat Model](#) -
[Contests - Untechnical](#) -
[Contests - DEF CON Scavenger Hunt](#) -
[Contests - Darknet-NG](#) -

[Contests - Crack Me If You Can 2026 -](#)
[Contests - TeleChallenge -](#)
[Contests - HackFortress -](#)
[Contests - ?Cube -](#)
[Contests - \\$unLight Sh4d0w5 -](#)
[Contests - Octopus Game - Booth Open -](#)
[Contests - Octopus Game Opens and Pre-registration Check-In Available -](#)
[Contests - Octopus Game - Opening Ceremony -](#)
[Contests - Beer Chilling Contraption Contest -](#)
[Contests - Cryptid Hunt -](#)
[Contests - HSPACE: AI Battlegrounds -](#)
[Contests - spyVspy 3: Rat Race -](#)
[Contests - Hacker Games -](#)
[Contests - PhreakMe -](#)
[Contests - Game Hacking Village CTF -](#)
[Contests - Kubernetes CTF -](#)
[Contests - Hac-Man -](#)
[Contests - Crack the Core -](#)
[Contests - Cyber Deck Competition -](#)
[Contests - Pinball High Score Contest -](#)
[Contests - Code Cadaver: Break Every System. Save Your Friend. -](#)
[Contests - PWN UR H0M3 - DDoS CTF -](#)
[Contests - Reali7y Overrun - Contest running -](#)
[Contests - Tin Foil Hat Contest -](#)
[Contests - CMD+CTRL Cyber Range: DarkMoney -](#)
[Contests - DEF CON CTF: Benevolent Bureau of Birds -](#)
[Contests - AI Village - Hal CTF -](#)
[Contests - AI Village Plays Pokemon: DEFCON Edition - Nick Ashworth](#)
[Contests - StarPWN CTF -](#)
[Contests - Car Hacking Village CTF -](#)
[Contests - OWASP CTF -](#)
[Contests - \(10:30-11:30 PDT\) - OWASP CTF: Getting started & welcome - Diego Cotel,Chris "dafinga" Maenner,Christian "DeadlyFluVirus" Nuss](#)
[Contests - Blue Team Village CTF - Project Obsidian -](#)
[Contests - Escalation Desk CTF -](#)
[Contests - DEF CON Groups Sticker Contest -](#)
[Contests - DEF CON Groups Backdoors & Breaches - Tim Doerges,Seth Benning](#)
[Contests - Apex Park \(Cloud Village CTF\) -](#)
[Contests - cont...\(09:00-11:59 PDT\) - SEC Vishing Competition \(SECVV\) -](#)
[Contests - Bug Bounty Village CTF - Open -](#)
[Contests - Hacking GRC Contest -](#)
[Crypto & Privacy Village - \(10:30-10:59 PDT\) - What TEEs Do Not Hide: Residual Metadata Leakage in Confidential LLM Serving - Anup Swamy Veena](#)
[Data Duplication Village - DDV open and accepting drives for duplication -](#)
[DCNextGen - \(10:30-11:30 PDT\) - DCNextGen Opening Ceremonies - BiaSciLab](#)
[DEF CON Groups - DEF CON Groups \(DCG\) -](#)
[DEF CON Talks - Car Hacking Village Scavenger Hunt Contest -](#)
[DEF CON Talks - Welcome to DEF CON 34! - Jeff "The Dark Tangent" Moss](#)
[DEF CON Talks - \(10:30-10:59 PDT\) - The DEF CON 34 Badge - Andrew 'bunnie' Huang](#)
[DEF CON Talks - Breaking the Ethereum Phone: From BootROM to Wallet Signing Keys - Guanxing Wen](#)
[DEF CON Talks - \(10:30-11:30 PDT\) - Breaking Local AI Runtimes: Exploiting llama.cpp and Ollama - Ofek Itach,Vladimir "G1ND1L4" Tokarev](#)
[DEF CON Talks - From square root to /root: escalating privileges in Azure containers with Python in Excel - Ron Ben Yizhak](#)
[DEF CON Talks - Weaponizing Uselessness: Breaking SMM with the Slowest Instruction Ever Written - Christopher "xoreaxeaxeax" Domas](#)

DEF CON Talks - (10:30-11:30 PDT) - [Reflections on Disregarding Trust \(Weaponizing CDP and MHTML for Header-Agnostic Session Hijacking\)](#) - Gregory "lumberhack" Disney-Leugers

DEF CON Talks - [Texas Incidents - How we broke the OMAP-L138 Trusted Execution Environment](#) - Carlo Meijer, Wouter Bokslag

DEF CON Training - cont...(08:30-17:30 PDT) - [Beat the Breach: Defend, Respond, Survive](#) - McKay Hardy, Wes Wagstaff

DEF CON Training - cont...(08:30-17:30 PDT) - [Cyber & AI Policy Basics: What Every Organization Needs in Place](#) - Pamela 'Pam' Feld, Greg Goldberg

DEF CON Training - cont...(08:30-17:30 PDT) - [Digital Supply Chain Security: Software, Cryptography, AI, and Vendor Risk](#) - Anant Shrivastava, Sunil Yadav

DEF CON Workshops - cont...(09:00-12:59 PDT) - [Sold Out - Offensive Packet Wizardry with Scapy](#) - Mike "Chicolinux" Guirao

DEF CON Workshops - cont...(09:00-12:59 PDT) - [Sold Out - Hands-on IoT firmware extraction and flash forensics](#) - Dennis Giese, Braelynn Luedtke, Arnold Wey, Harsha Potu

DEF CON Workshops - cont...(09:00-12:59 PDT) - [Sold Out - AWS Cloud Security 101: From IAM Misconfigurations to Account Takeover](#) - zeta, Rafa "bane" Gutierrez

DEF CON Workshops - cont...(09:00-12:59 PDT) - [Sold Out - Web Hacking 101](#) - cale "calebot" smith, Ruchik Dave, Young Seuk Kim, Luke Cycon

DEF CON Workshops - cont...(09:00-12:59 PDT) - [Sold Out - Malware Development 101 - From Zero to Hero: Adapt your payload to your environment](#) - Yoann "OtterHacker" DEQUEKER

DEF CON Workshops - cont...(09:00-12:59 PDT) - [Sold Out - Long Live Empire: A C2 Workshop for Modern Red Teaming](#) - Jake "Hubbl3" Krasnov, Vincent "Vinnybod" Rose, Anthony "Coin" Rose, Dan Niefeld

DEF CON Workshops - cont...(09:00-12:59 PDT) - [Sold Out - Learning to Hack Bluetooth Low Energy with BLE CTF](#) - Ryan "Hackgnar" Holeman, Alek Amrani

DEF CON Workshops - cont...(09:00-12:59 PDT) - [Sold Out - Agentic Threat Hunting: Building AI That Remembers What You Hunted](#) - Sydney "letswastetime" Marrone

Demo Labs - [AD-Necromancer: Resurrecting Forgotten Control Paths in Active Directory](#) - Akbar "0xsensei" Abdullayev, 0xHera

Demo Labs - [Peekaboo: Breaking the Black Box of Threat and Malware Emulation](#) - Zhassulan "cocomelonc" Zhussupov

Demo Labs - [Senrigan \(\) x Suzaku \(\) : Threat Hunting & DFIR for AWS — No SIEM, Just Your Laptop](#) - Fukusuke Takahashi, Zach Mathis, Akira Nishikawa

Demo Labs - [X-Ray Your Agents: Pentesting MCPs, Skills, and the Plugin Supply Chain](#) - Xia Hua, Abhijeet Kumar

Demo Labs - [PromptPwn: Finding and Exploiting AI-Generated Vulnerabilities at Scale](#) - Georgia Weidman

Demo Labs - [Empire 7: Shipping a C2 at AI Speed](#) - Vincent "Vinnybod" Rose, Jake "Hubbl3" Krasnov, Anthony "Coin" Rose

Embedded Systems Village - [Embedded - 101 Labs](#) -

Embedded Systems Village - [Embedded Systems Village CTF](#) -

Embedded Systems Village - [Exploit Bluetooth Low Energy with BLESPlloit and optional ESP32](#) - Slawomir Jasek

Game Hacking Village - [Chill Zone: Casual Games & TASBot Smash Demo](#) -

IoT Village - [All About UART](#) -

IoT Village - [Just Hacking Training](#) -

IoT Village - [Discover GE Appliances!](#) -

IoT Village - [Cat-astrophic Hacking: Breaking Into Smart Litter Boxes](#) -

IoT Village - [Raiders of the Lost Firmware: A Hands-On Workshop in IoT Firmware Archaeology](#) -

IoT Village - [Hands-On Hardware Hacking – From JTAG to Root, Memory Patching Boot Process for Root Access](#) -

IoT Village - [Expose Hidden Surveillance in Everyday Tech](#) -

IoT Village - [Smart Home in the Matter: Blink, Race, Attack CTF](#) -

IoT Village - (10:30-11:30 PDT) - [Make your very own evil IoT Cat Lamp with WLED!](#) - Nick

IoT Village - (10:45-11:30 PDT) - [Sick Signals: Adversarial Prompt Injection via Medical IoT Telemetry](#) - Vinitha Mathiyazhagan, Tamil Mathi T.

La Villa Community - [La Villa - Opening Ceremony \(ESP\)](#) -

La Villa Community - (10:30-11:30 PDT) - [Bootkits Forever: Emulando APTs Modernos desde UEFI hasta el Kernel](#) - Alejandro Vázquez Vázquez

La Villa Community - (10:30-12:59 PDT) - [De la nube a la corona: Uso indebido de la identidad híbrida en Azure DevOps Azure, AD, AWS y EKS](#) - Juan Camilo Palacio Arango, Andrés Restrepo

Lockpick Village - (10:15-10:45 PDT) - [Intro to Lockpicking](#) -

Lonely Hackers Club - [Lonely Hackers Club](#) - [Sticker Swap Table](#) -

Lonely Hackers Club - Lonely Hackers Club - Lockpicking Table -
 Lonely Hackers Club - Lonely Hackers Club CTF -
 Lonely Hackers Club - (10:30-16:30 PDT) - Resume Review with the Lonely Hackers Club -
 Maker's Village - Makers' Village - Hacker Arts and Crafts -
 Malware Village - Anatomy of a Sandworm: A Deep Dive into the Shai-Hulud Attacks - Megg Sage
 Malware Village - (10:55-11:35 PDT) - Lyra: An LLVM IR Obfuscator for Rust - Rafael Felix
 Malware Village - The Silent Tunnel: A Real-World Incident Response Story - Uriel Kosayev
 Maritime Hacking Village - Maritime Hacking Village Policy Panel: Subsea Cables as Strategic Chokepoints - Security, Sovereignty, and the Grey Zone - Dr. Nina Kollars, Jason Vogt, Delta Blue
 Misc - Coloring Reset -
 Mobile Hacking Community - Mobile Hacking Community - Open -
 Mobile Hacking Community - Bypassing KYC Vendors on AI Times - Juan Urbano Stordeur, Juan Martinez Blanco
 Mobile Hacking Community - Mobile Hacking - Informal CTF -
 Nix Vegas Community - Nix Vegas Opening Ceremony - Daniel Baker, Morgan Jones, Tristan Ross
 Nix Vegas Community - (10:30-10:59 PDT) - Composable Systems with NixOS MicroVMs - Alex Decious
 Noob Community - TCM Security Labs -
 Noob Community - Skillbit Labs -
 Noob Community - SANS Institute NetWars Labs -
 Noob Community - Arcanum Security Labs -
 Noob Community - Kryptsec Labs -
 Noob Community - Hack The Box DC Junior Ranger Program Challenge -
 Noob Community - Mentoring and Career Advice -
 Noob Community - No Stupid Questions -
 Noob Community - Noob Community - DEF CON 34 Opening Statements -
 Noob Community - Practical Cybersecurity Skills in an AI-Augmented World: Protecting the AI Trifecta - James Stanger, Stephen Schneider
 OSINT For Good Community - OSINT4Good: What it takes to find missing people - Angela Ramos, Kenny J, Brent Louie
 OSINT For Good Community - OSINT4Good Community - DC NextGen Content -
 OSINT For Good Community - FINDX OSINT Educational Series -
 OWASP Foundation - BadVR: Signals Everywhere a collaboration with XR Village - Jad Meouchy, Suzanne Borders
 Payment Village - (10:45-11:30 PDT) - The Future of Payments: AI, Agentic Commerce and the Next Wave of Innovation - Daniel Cuthbert, Leigh-Anne Galloway, Jorge Braniff, Sanjeev Sharma
 Payment Village - (10:30-10:45 PDT) - Payment Village Intro - What's Happening at the Village -
 Policy @ DEF CON - Sovereign by Design, Vulnerable by Default - Devin Lynch, Haley Ring
 Policy @ DEF CON - Not Your Parents' Schoolhouse Rock: Getting Tech Policy Done in a Non-Functioning Congress - Jeff Rothblum, Michael Flynn
 Radio Frequency Village - Radio Frequency Village Events -
 Radio Frequency Village - (10:30-12:25 PDT) - RF CTF Kick Off Day 1 - RF Hackers
 Recon Village - Hands-On Supply Chain Recon & Vendor Risk Mapping - Dhiyaneshwaran Balasubramaniam, Aman Rawat
 Recon Village - TrackTheFugitive Contest -
 Recon Village - Live Recon Contest -
 Recon Village - (10:45-11:30 PDT) - InQuorigible: Quora in Missing Persons OSINT - Miranda Tedholm
 Red Team Village - From Kiosk to Domain Compromise: Learning to Walk Up and Take it All - Ezra Woods, Mike Manrod, Spencer Alessi
 Red Team Village - BloodHound Quest - Hugo van den Toorn
 Red Team Village - Post-Exploitation of the Desktop with JS-Tap - Drew Kirkpatrick
 Red Team Village - Red Team Express - Cody Spooner
 Red Team Village - Zero Signal: Operating Where Defenders Can't See - Gowthamaraj Rajendran
 Red Team Village - Falco Hunt: Evading Runtime Detection in Kubernetes - Michael Reimsbach
 Red Team Village - Opening Panel - "Is Red Teaming Dead?" - Ads Dawson, Ben "NahamSec" Sadeghipour, Billy Giles, Ryan Montgomery
 Red Team Village - The Entropy Illusion: High-Speed Cracking on a Budget - Chris Claunch
 Red Team Village - RFID Bootcamp: Unleashed! - Evan Cook
 Scambait Village - KSCM Scambait Radio -
 Scambait Village - Open Q&A -

[Social Engineering Community Village](#) - cont...(08:30-17:59 PDT) - [Social Engineering Community Village - Open Hours](#) - [Social Engineering Community Village - Pickpocketing for Red Teamers: A Hands-On Experience](#) - pradameinhof

[Social Gatherings/Events](#) - cont...(08:00-18:59 PDT) - [Human Registration Open](#) -

[Social Gatherings/Events - Malysis: A Bare-Metal RAM Enclave for Malware Analysis. No Hypervisor. No Trace.](#) - Yannick LaRue,Samuel B. G.

[Social Gatherings/Events - Malysis: A Bare-Metal RAM Enclave for Malware Analysis. No Hypervisor. No Trace.](#) - Yannick LaRue,Samuel B. G.

[Social Gatherings/Events](#) - cont...(08:00-17:59 PDT) - [Merch \(formerly swag\) Area Open -- README](#) -

[Social Gatherings/Events - Music - SomaFM](#) -

[Social Gatherings/Events](#) - cont...(06:00-10:59 PDT) - [15th Cycleoverride Bike Ride at DEF CON](#) -

[Telecom Village - Telecom Village Inauguration](#) - Pankaj Sontakke

[Telecom Village - \(10:20-10:59 PDT\) - A 5G Digital Twin CTF for Hacking Carrier-Grade Infrastructure](#) - Siva Sareddu,T -Mobile CTF Team

[The Diana Initiative - IOT Village Tour](#) -

[The Diana Initiative - \(10:20-10:30 PDT\) - Quantum Village Tour](#) -

[The Diana Initiative - \(10:30-10:40 PDT\) - AppSec Village Tour](#) -

[The Diana Initiative - \(10:40-10:50 PDT\) - Robot Hacking Community Tour](#) -

[The Diana Initiative - \(10:50-10:59 PDT\) - Physical Securty Village Tour](#) -

[The Diana Initiative - Quiet Room](#) -

[The Diana Initiative - Hacker Runway Crafting Time](#) -

[Voting Village - Voting Village Lab](#) -

[Voting Village - Election Integrity and Technology](#) - Matt Blaze

[Voting Village - \(10:30-10:59 PDT\) - What Election Security Researchers Need to Know About the DMCA](#) - Tori Noble

[.EDU Community](#) - [Cracking the Cybersecurity Career Code with the Cyber Color Wheel](#) - Shavvon "TheSiren" Cintron

[Adversary Village](#) - (11:30-11:59 PDT) - [Haetae: An Agent to Takedown North Korean C2 Servers](#) - Mauro Eldritch,Nelson Rafael Colón Merán

[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Satellites Under Attack: Hands-On Satellite Security Threat Scenarios](#) -

[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Nebula Showdown: Space Systems Security CTF Adventure](#) -

[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [SR-71 Blackbird Badge Challenge](#) -

[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [SpaceCOP - Catch Me If You Can](#) -

[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Drone Hacking Workshop](#) -

[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Mission: Compromised - Hacking a Satellite from the Ground Up](#) -

[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [MOUSE Runner & Flappy Drone](#) -

[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Flight Simulator/EFB](#) -

[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Aviation ISAC Cybersecurity Challenge](#) -

[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Aerospace Ecosystem Resilience Innovation Environment \(AERIE\) Cyber Range](#) -

[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [ARINC 664 CTF Challenge](#) -

[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Drone Hacking Choose your Own Adventure](#) -

[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [DCNextGen - Space Grand Challenge - SatHack: The MOUSE-1 Mission](#) -

[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [DCNextGen - RIC-1: ELT Localization Exercise - N3VR-G0N Down](#) -

[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [DCNextGen - Bricks in the Air](#) -

[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Bricks in the Air](#) -

[AI Village](#) - cont...(10:00-17:59 PDT) - [AI Village: Village Open](#) -

[AI Village](#) - cont...(10:00-17:59 PDT) - [Poster Presentations](#) -

[AI Village](#) - cont...(10:00-17:59 PDT) - [Cyber Mirage: Realtime Deepfake Demos](#) - Brandon Kovacs

[AppSec Village](#) - cont...(10:15-11:15 PDT) - [Pentesting made easy - Keeping sessions alive with session chains](#) - Kai Glauber,Matthias Göhring

[AppSec Village](#) - (11:30-12:30 PDT) - [Aegis of the Vulnerable: A Unified Pipeline for AI-Based SAST](#) - Can Oztas

[AppSec Village](#) - cont...(10:30-12:30 PDT) - [Burp, But Yours: Hands-On Extension and Bambda Development](#) - Hannah L

[AppSec Village](#) - [Pickled and Exposed: RCE in AI Serving Frameworks](#) - Iggy

[AppSec Village](#) - (11:50-12:20 PDT) - [A Billion-User Blast Radius: Owning ChatGPT's Secure Sandbox](#) - Simcha Kosman

[AppSec Village](#) - [Cards Against Vulnerabilities](#) - Patrick Smyth

[AppSec Village](#) - [The Call Stack Experience](#) - Victoria Keeler

[AppSec Village](#) - [Clash of Prompts: The World's First Prompt Battle Royale](#) -

[AppSec Village](#) - [Hack the Duck Store](#) - Gwendal Mognier,Samantha Pearlstein

[Biohacking Village](#) - cont...(10:00-17:59 PDT) - [Biohacking Device Lab](#) -

[Biohacking Village](#) - cont...(10:00-17:59 PDT) - [Embedded & Shredded: Advanced Embedded System Hacking](#) -

[Biohacking Village](#) - (11:30-11:59 PDT) - [Human in the Loop or Human Out of Luck?](#) - Christine Von Raesfeld

[Blacks In Cyber Village](#) - [The Black PhD Playbook: What No One Tells You](#) - Dr. Fatou Sankare,Dr. Xavier-Lewis Palmer,Dr. Tia Pope

[Blue Team Village](#) - [Cyber Threat Intelligence 101: From Foundations to AI-Driven Defense](#) - Carlo Anez Mazurco

[Bug Bounty Village](#) - [The Ripple Effect: Inside Cloud-Scale Vulnerabilities in the Age of AI](#) - Albin Vattakattu,Ryan Nolette

[Bug Bounty Village](#) - (11:30-11:59 PDT) - [Make Money Hacking AI](#) - Joey Melo,Edward Morris

[Bug Bounty Village](#) - cont...(10:30-11:30 PDT) - [Hacking IDE Extensions - VSCode Workshop](#) - Nick "7urb01" Copi

[Bug Bounty Village](#) - (11:30-12:30 PDT) - [Hackbots](#) - Jason "jhaddix" Haddix,Ryan "BadAt_Computers" Bonner

[Call Center Village](#) - cont...(10:00-17:59 PDT) - [Call Center Village - Open](#) -

[Car Hacking Village](#) - cont...(10:00-17:59 PDT) - [Car Hacking Village Open](#) -

[Car Hacking Village](#) - cont...(10:00-16:59 PDT) - [Bomb Bot Challenge](#) -

[Cloud Village](#) - [Weaponizing CloudFormation: Privilege Escalation via Infrastructure as Code in AWS](#) - Samanta Aranda

[Cloud Village](#) - [Governing the Firehose: Writing Custom OPA Policies to Tame and Remediate Prowler Output](#) - Ram "n2r"

[Cloud Village](#) - cont...(10:50-11:30 PDT) - [Tokens and PRT: Advanced Attacks and Persistence in Microsoft Entra ID](#) - Elzer Pineda,Jose Rivas

[Cloud Village](#) - (11:30-12:10 PDT) - [From Pipeline to Cloud Control](#) - Saksham Agrawal

[CodeBloom](#) - [Work Session: Ciphers](#) -
[Contests](#) - cont...(10:00-12:59 PDT) - [Aw, man...pages!](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [5N4CK3Y](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [DC's Next Top Threat Model](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Untechnical](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [DEF CON Scavenger Hunt](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Darknet-NG](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Crack Me If You Can 2026](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [TeleChallenge](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [HackFortress](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [?Cube](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [\\$unLight Sh4d0w5](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Octopus Game - Booth Open](#) -
[Contests](#) - cont...(10:00-12:59 PDT) - [Octopus Game Opens and Pre-registration Check-In Available](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Beer Chilling Contraption Contest](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Cryptid Hunt](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [HSPACE: AI Battlegrounds](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [spyVspy 3: Rat Race](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Hacker Games](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [PhreakMe](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Game Hacking Village CTF](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Kubernetes CTF](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Hac-Man](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Crack the Core](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Cyber Deck Competition](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Pinball High Score Contest](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Code Cadaver: Break Every System. Save Your Friend.](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [PWN UR H0M3 - DDoS CTF](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Real7y Overrun - Contest running](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Tin Foil Hat Contest](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [CMD+CTRL Cyber Range: DarkMoney](#) -
[Contests](#) - [Radio Frequency Capture the Flag](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [DEF CON CTF: Benevolent Bureau of Birds](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [AI Village Plays Pokemon: DEFCON Edition](#) - Nick Ashworth
[Contests](#) - cont...(10:00-17:59 PDT) - [AI Village - Hal CTF](#) -
[Contests](#) - cont...(10:00-11:59 PDT) - [StarPWN CTF](#) -
[Contests](#) - cont...(10:00-16:59 PDT) - [Car Hacking Village CTF](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [OWASP CTF](#) -
[Contests](#) - cont...(10:30-11:30 PDT) - [OWASP CTF: Getting started & welcome](#) - Diego Cotel,Chris "dafinga"
Maenner,Christian "DeadlyFluVirus" Nuss
[Contests](#) - cont...(10:00-11:59 PDT) - [Blue Team Village CTF - Project Obsidian](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Escalation Desk CTF](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [DEF CON Groups Sticker Contest](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [DEF CON Groups Backdoors & Breaches](#) - Tim Doerges,Seth Benning
[Contests](#) - cont...(10:00-23:59 PDT) - [Apex Park \(Cloud Village CTF\)](#) -
[Contests](#) - cont...(09:00-11:59 PDT) - [SEC Vishing Competition \(SECVV\)](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Hacking GRC Contest](#) -
[Contests](#) - [Radio Frequency Capture the Flag](#) -
[Cryptocurrency Village](#) - [Cryptocurrency Opening Keynote](#) - Michael "MsvB" Schloh,Param "P7R7M",Arjun "Peper" Suresh
[Data Duplication Village](#) - cont...(10:00-17:59 PDT) - [DDV open and accepting drives for duplication](#) -
[Data Duplication Village](#) - [Drive Stats: 14 years of hard drive failure rates](#) - Stephanie Doyle
[DCNextGen](#) - cont...(10:30-11:30 PDT) - [DCNextGen Opening Ceremonies](#) - BiaSciLab
[DEF CON Groups](#) - (11:30-11:59 PDT) - [Starting and Sustaining a Successful DEF CON Group presented by DC862](#) - C\$,Joe
Folk,Christopher "reapermunky" Aziz
[DEF CON Groups](#) - cont...(10:00-17:59 PDT) - [DEF CON Groups \(DCG\)](#) -

DEF CON Talks - cont...(10:00-11:59 PDT) - [Car Hacking Village Scavenger Hunt Contest](#) - Ian Roos, Mark Trumbour

DEF CON Talks - cont...(10:30-11:30 PDT) - [Breaking Local AI Runtimes: Exploiting llama.cpp and Ollama](#) - Ofek Itach, Vladimir "G1ND1L4" Tokarev

DEF CON Talks - (11:30-12:30 PDT) - [Crashing the Party: Pwning Control-Flow Integrity with Segmentation Fault-Oriented Programming](#) - Marcos "h3xduck" Bajo, Ritvik "RoYalGamr" Goyal

DEF CON Talks - [Sliding into the Flight Deck's DMs: Practical Message Attacks on CPDLC](#) - Martin "MasorX" Strohmeier, Mehdi Ziazi

DEF CON Talks - cont...(10:30-11:30 PDT) - [Reflections on Disregarding Trust \(Weaponizing CDP and MHTML for Header-Agnostic Session Hijacking\)](#) - Gregory "lumberhack" Disney-Leugers

DEF CON Talks - (11:30-12:30 PDT) - [A Provider for the MOFia - Distributed Post-Ex Capabilities](#) - Steven Flores

DEF CON Talks - [Keychained Melody - Grabbing the Keys to the iCloud Kingdom](#) - Alex Radocea, Jaron Bradley

DEF CON Training - cont...(08:30-17:30 PDT) - [Beat the Breach: Defend, Respond, Survive](#) - McKay Hardy, Wes Wagstaff

DEF CON Training - cont...(08:30-17:30 PDT) - [Cyber & AI Policy Basics: What Every Organization Needs in Place](#) - Pamela 'Pam' Feld, Greg Goldberg

DEF CON Training - cont...(08:30-17:30 PDT) - [Digital Supply Chain Security: Software, Cryptography, AI, and Vendor Risk](#) - Anant Shrivastava, Sunil Yadav

DEF CON Workshops - cont...(09:00-12:59 PDT) - [Sold Out - Offensive Packet Wizardry with Scapy](#) - Mike "Chicolinux" Guirao

DEF CON Workshops - cont...(09:00-12:59 PDT) - [Sold Out - Hands-on IoT firmware extraction and flash forensics](#) - Dennis Giese, Braelynn Luedtke, Arnold Wey, Harsha Potu

DEF CON Workshops - cont...(09:00-12:59 PDT) - [Sold Out - AWS Cloud Security 101: From IAM Misconfigurations to Account Takeover](#) - zeta, Rafa "bane" Gutierrez

DEF CON Workshops - cont...(09:00-12:59 PDT) - [Sold Out - Web Hacking 101](#) - cale "calebot" smith, Ruchik Dave, Young Seuk Kim, Luke Cycon

DEF CON Workshops - cont...(09:00-12:59 PDT) - [Sold Out - Malware Development 101 - From Zero to Hero: Adapt your payload to your environment](#) - Yoann "OtterHacker" DEQUEKER

DEF CON Workshops - cont...(09:00-12:59 PDT) - [Sold Out - Long Live Empire: A C2 Workshop for Modern Red Teaming](#) - Jake "Hubbl3" Krasnov, Vincent "Vinnybod" Rose, Anthony "Coin" Rose, Dan Niefeld

DEF CON Workshops - cont...(09:00-12:59 PDT) - [Sold Out - Learning to Hack Bluetooth Low Energy with BLE CTF](#) - Ryan "Hackgnar" Holeman, Alek Amrani

DEF CON Workshops - cont...(09:00-12:59 PDT) - [Sold Out - Agentic Threat Hunting: Building AI That Remembers What You Hunted](#) - Sydney "letswastetime" Marrone

Demo Labs - [Damn Vulnerable Agentic AI Application \(DVAIA\)](#) - Abhinav Verma, Mukesh Aggarwal

Demo Labs - [sisakulint: CI-Friendly static linter with autofix, SAST, semantic analysis for GitHub Actions](#) - Atsushi Sada, hikae

Demo Labs - [Be like a BRAT\(BLE Recon and Attack Toolkit\): Skip the Handshake, Own the Device](#) - Gigi Xiaoping Liu, Muzzammil Mohammed, Narmina Karimova

Demo Labs - [Zealot: An Autonomous Cloud Offensive Multi-Agent System](#) - Chen Doytshman

Demo Labs - [AOBTD: AI One Bites The DAST](#) - Ozgun "ozzy" Kultekin

Demo Labs - [AI Pipeline for N-days Weaponization](#) - Andrea Brosio, Arun Nair

Embedded Systems Village - cont...(10:00-17:59 PDT) - [Embedded - 101 Labs](#) - Embedded Systems Village

Embedded Systems Village - cont...(10:00-17:59 PDT) - [Embedded Systems Village CTF](#) - Embedded Systems Village

Embedded Systems Village - cont...(10:00-17:59 PDT) - [Exploit Bluetooth Low Energy with BLESPlloit and optional ESP32](#) - Slawomir Jasek

Game Hacking Village - cont...(10:00-15:59 PDT) - [Chill Zone: Casual Games & TASBot Smash Demo](#) - Hackers.town

Hackers.town - [Tech Reclaimers Update: A Year In, Building a Social Movement Away from Big Tech](#) - Andy Hull, Janet Vertesi, Rebecah Miller

Hackers.town - [building community and privacy tools from junk](#) - TheGibson

Ham Radio Village - [Meshtastic 101: Off-Grid Mesh Networking with LoRa](#) - Jon Marler (K4CHN)

ICS Village - [Intro to Common Industrial Protocol Exploitation](#) - Trevor Flynn

IoT Village - cont...(10:00-17:59 PDT) - [All About UART](#) - IoT Village

IoT Village - cont...(10:00-17:59 PDT) - [Discover GE Appliances!](#) - IoT Village

IoT Village - cont...(10:00-17:59 PDT) - [Cat-astrophic Hacking: Breaking Into Smart Litter Boxes](#) - IoT Village

IoT Village - cont...(10:00-17:59 PDT) - [Raiders of the Lost Firmware: A Hands-On Workshop in IoT Firmware Archaeology](#)

-

IoT Village - cont...(10:00-17:59 PDT) - [Hands-On Hardware Hacking – From JTAG to Root, Memory Patching Boot Process for Root Access](#) -

IoT Village - cont...(10:00-17:59 PDT) - [Just Hacking Training](#) -

IoT Village - cont...(10:00-17:59 PDT) - [Expose Hidden Surveillance in Everyday Tech](#) -

IoT Village - cont...(10:00-17:59 PDT) - [Smart Home in the Matter: Blink, Race, Attack CTF](#) -

IoT Village - cont...(10:30-11:30 PDT) - [Make your very own evil IoT Cat Lamp with WLED!](#) - Nick

IoT Village - cont...(10:45-11:30 PDT) - [Sick Signals: Adversarial Prompt Injection via Medical IoT Telemetry](#) - Vinitha Mathiyazhagan,Tamil Mathi T.

La Villa Community - cont...(10:30-11:30 PDT) - [Bootkits Forever: Emulando APTs Modernos desde UEFI hasta el Kernel](#) - Alejandro Vázquez Vázquez

La Villa Community - (11:30-12:30 PDT) - [Demodus Operandi \(Cómo tres rf-hacks en tres bandas terminaron siendo una metodología\)](#) - Eduardo Contreras

La Villa Community - cont...(10:30-12:59 PDT) - [De la nube a la corona: Uso indebido de la identidad híbrida en Azure DevOps Azure, AD, AWS y EKS](#) - Juan Camilo Palacio Arango,Andrés Restrepo

Lockpick Village - [Building an open source safecracking robot](#) - Jared Dygert

Lonely Hackers Club - cont...(10:00-17:59 PDT) - [Lonely Hackers Club CTF](#) -

Lonely Hackers Club - cont...(10:00-17:59 PDT) - [Lonely Hackers Club - Sticker Swap Table](#) -

Lonely Hackers Club - cont...(10:00-17:59 PDT) - [Lonely Hackers Club - Lockpicking Table](#) -

Lonely Hackers Club - cont...(10:30-16:30 PDT) - [Resume Review with the Lonely Hackers Club](#) -

Maker's Village - cont...(10:00-17:59 PDT) - [Makers' Village - Hacker Arts and Crafts](#) -

Maker's Village - [Build-A-Badge Workshop](#) - hunny,Teazee,Buddha,MLP,M-Nelly,Alchemmer

Malware Village - cont...(10:55-11:35 PDT) - [Lyra: An LLVM IR Obfuscator for Rust](#) - Rafael Felix

Malware Village - cont...(10:10-11:40 PDT) - [The Silent Tunneler: A Real-World Incident Response Story](#) - Uriel Kosayev

Maritime Hacking Village - (11:30-12:15 PDT) - [Building the Humans Behind the Mission: Talent, Readiness, and Cyber Power for America's Armed Services](#) - Dr. Nina Kollars,Dr. Wanda T. Jones-Heath,Anne Marie Schumann

Middle Easterns & Africans in Cyber Security (MEACS) - [Logsquashing: Consolidating Relevant Events Logs and Alerts](#) - Ezz Tahoun

Mobile Hacking Community - cont...(10:00-17:59 PDT) - [Mobile Hacking Community - Open](#) -

Mobile Hacking Community - cont...(10:00-17:59 PDT) - [Mobile Hacking - Informal CTF](#) -

Mobile Hacking Community - [AI finds and writes my Android exploits now](#) - Ken Gannon /

Nix Vegas Community - (11:30-11:59 PDT) - [Running a homelab with NixOS](#) - Aaron Honeycutt

Noob Community - cont...(10:00-17:59 PDT) - [Mentoring and Career Advice](#) -

Noob Community - cont...(10:00-17:59 PDT) - [Hack The Box DC Junior Ranger Program Challenge](#) -

Noob Community - cont...(10:00-17:59 PDT) - [No Stupid Questions](#) -

Noob Community - cont...(10:00-17:59 PDT) - [Arcanum Security Labs](#) -

Noob Community - cont...(10:00-17:59 PDT) - [Kryptsec Labs](#) -

Noob Community - cont...(10:00-17:59 PDT) - [Skillbit Labs](#) -

Noob Community - cont...(10:00-17:59 PDT) - [TCM Security Labs](#) -

Noob Community - cont...(10:00-17:59 PDT) - [SANS Institute NetWars Labs](#) -

Noob Community - cont...(10:00-13:50 PDT) - [Practical Cybersecurity Skills in an AI-Augmented World: Protecting the AI Trifecta](#) - James Stanger,Stephen Schneiter

Noob Community - [Privilege Escalation: A Career Story](#) - Ryan Bonner,Whit Taylor

Noob Community - (11:45-12:45 PDT) - [If I Were Eighteen Again: Career Advice for the AI Era](#) - Keith Hoodlet

OSINT For Good Community - cont...(10:00-17:59 PDT) - [OSINT4Good Community - DC NextGen Content](#) -

OSINT For Good Community - cont...(10:00-17:59 PDT) - [FINDX OSINT Educational Series](#) -

OSINT For Good Community - [Q&A with the OSINT4Good Panel](#) - Angela Ramos,Kenny J,Brent Louie

OSINT For Good Community - (11:45-12:15 PDT) - [Welcome to OSINT4Good and Trace Labs](#) - Nataly "someone_somewhere"

OWASP Foundation - cont...(10:00-17:59 PDT) - [BadVR: Signals Everywhere a collaboration with XR Village](#) - Jad Meouchy,Suzanne Borders

OWASP Foundation - (11:30-11:59 PDT) - [Spotlight: Choose Your Own Adventure with InfoSecMap](#) - W. Martín Villalba

Payment Village - cont...(10:45-11:30 PDT) - [The Future of Payments: AI, Agentic Commerce and the Next Wave of Innovation](#) - Daniel Cuthbert,Leigh-Anne Galloway,Jorge Braniff,Sanjeev Sharma

Payment Village - [A Real-Time Battle with a Card-Testing Adversary](#) - Levi Schuck

Payment Village - (11:30-11:50 PDT) - [Introduction to Vulnerable ATM Badge](#) - Vincent Sloan
 Policy @ DEF CON - [Morbidity and Mortality: Hackers, HIPAA, and a new Prescription for Healthcare Cyber Policy](#) - Christian Dameff, Jeff "r3plicant" Tully
 Queercon Community - [Trans Townhall](#) -
 Radio Frequency Village - cont...(10:00-17:59 PDT) - [Radio Frequency Village Events](#) -
 Radio Frequency Village - cont...(10:30-12:25 PDT) - [RF CTF Kick Off Day 1](#) - RF Hackers
 Recon Village - cont...(10:00-12:30 PDT) - [Hands-On Supply Chain Recon & Vendor Risk Mapping](#) - Dhiyaneshwaran Balasubramaniam, Aman Rawat
 Recon Village - cont...(10:00-23:59 PDT) - [Live Recon Contest](#) -
 Recon Village - cont...(10:00-23:59 PDT) - [TrackTheFugitive Contest](#) -
 Recon Village - [GE\(O\)SINT Contest](#) -
 Recon Village - cont...(10:45-11:30 PDT) - [InQuorigible: Quora in Missing Persons OSINT](#) - Miranda Tedholm
 Red Team Village - cont...(10:00-17:59 PDT) - [From Kiosk to Domain Compromise: Learning to Walk Up and Take it All](#) - Ezra Woods, Mike Manrod, Spencer Alessi
 Red Team Village - cont...(10:00-17:59 PDT) - [BloodHound Quest](#) - Hugo van den Toorn
 Red Team Village - cont...(10:00-11:59 PDT) - [Post-Exploitation of the Desktop with JS-Tap](#) - Drew Kirkpatrick
 Red Team Village - cont...(10:00-11:59 PDT) - [Red Team Express](#) - Cody Spooner
 Red Team Village - cont...(10:00-11:59 PDT) - [Zero Signal: Operating Where Defenders Can't See](#) - Gowthamaraj Rajendran
 Red Team Village - cont...(10:00-11:59 PDT) - [Falco Hunt: Evading Runtime Detection in Kubernetes](#) - Michael Reimsbach
 Red Team Village - [Trusted Launcher, Untrusted Code: Weaponizing AppLaunch.exe to bypass SmartScreen and AppLocker](#) - Nathan Sawyer
 Red Team Village - [COM Hijacking Voodoo: Tradecraft, Detection Blind Spots, and the COM-Hunter](#) - Nikos "nickvourd" Vourdas
 Red Team Village - [Exploiting Private 5G: Unauthenticated Access to Databases and Control Plane DoS via Fuzzing](#) - Aumkareshwar DS
 Red Team Village - cont...(10:00-11:59 PDT) - [RFID Bootcamp: Unleashed!](#) - Evan Cook
 Scambait Village - cont...(10:00-17:59 PDT) - [Open Q&A](#) -
 Scambait Village - cont...(10:00-17:59 PDT) - [KSCM Scambait Radio](#) -
 Scambait Village - (11:30-13:59 PDT) - [Live Calls Workshop](#) -
 Social Engineering Community Village - cont...(08:30-17:59 PDT) - [Social Engineering Community Village - Open Hours](#) -
 Social Engineering Community Village - cont...(10:00-11:30 PDT) - [Pickpocketing for Red Teamers: A Hands-On Experience](#) - pradameinhof
 Social Gatherings/Events - cont...(08:00-18:59 PDT) - [Human Registration Open](#) -
 Social Gatherings/Events - cont...(10:00-16:59 PDT) - [Malysis: A Bare-Metal RAM Enclave for Malware Analysis. No Hypervisor. No Trace.](#) - Yannick LaRue, Samuel B. G.
 Social Gatherings/Events - cont...(10:00-16:59 PDT) - [Malysis: A Bare-Metal RAM Enclave for Malware Analysis. No Hypervisor. No Trace.](#) - Yannick LaRue, Samuel B. G.
 Social Gatherings/Events - [Book Signing - Nicholas DeMeo](#) - Nicholas DeMeo
 Social Gatherings/Events - [Book Signing - Christopher DeCarmen](#) - Christopher DeCarmen
 Social Gatherings/Events - cont...(08:00-17:59 PDT) - [Merch \(formerly swag\) Area Open -- README](#) -
 Social Gatherings/Events - cont...(10:00-18:59 PDT) - [Music - SomaFM](#) -
 Telecom Village - [SOC Threat Hunting in Practice](#) - Akib Sayyed
 The Diana Initiative - [Ham Radio Village Tour](#) -
 The Diana Initiative - [Packet Hacking Village Tour](#) -
 The Diana Initiative - (11:20-11:30 PDT) - [Mobile Hacking Tour](#) -
 The Diana Initiative - (11:30-11:40 PDT) - [Maritime Hacking Village Tour](#) -
 The Diana Initiative - (11:40-11:50 PDT) - [HHV/SSV Tour](#) -
 The Diana Initiative - (11:50-11:59 PDT) - [ICS Village Tour](#) -
 The Diana Initiative - cont...(10:00-11:59 PDT) - [Hacker Runway Crafting Time](#) -
 Voting Village - cont...(10:00-17:59 PDT) - [Voting Village Lab](#) -
 Voting Village - [Anomalies Are Not Normal: Election Foam Strikes and the Tragic Story of Mikey Hicks](#) - Richard DeMillo
 Voting Village - (11:30-11:59 PDT) - [Welcome to the Voting Village](#) - Brian DeMuth, Matt Blaze, Jake Braun, David Jefferson, Jeff Moss, Kendall Spencer, Philip Stark

[.EDU Community](#) - [Student-Run Cyber Clubs - Why They Matter & Digital Playgrounds](#) - Steven "Stengo" Ngo
[Adversary Village](#) - [Yet Another Walking Dead of Active Directory](#) - Nikos "nickvourd" Vourdas
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [ARINC 664 CTF Challenge](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Aerospace Ecosystem Resilience Innovation Environment \(AERIE\) Cyber Range](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Drone Hacking Choose your Own Adventure](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [DCNextGen - Space Grand Challenge - SatHack: The MOUSE-1 Mission](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [DCNextGen - RIC-1: ELT Localization Exercise - N3VR-G0N Down](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Aviation ISAC Cybersecurity Challenge](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [DCNextGen - Bricks in the Air](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Bricks in the Air](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Nebula Showdown: Space Systems Security CTF Adventure](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Satellites Under Attack: Hands-On Satellite Security Threat Scenarios](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [SR-71 Blackbird Badge Challenge](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [SpaceCOP - Catch Me If You Can](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Mission: Compromised - Hacking a Satellite from the Ground Up](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [MOUSE Runner & Flappy Drone](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Flight Simulator/EFB](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Drone Hacking Workshop](#) -
[Aerospace Village](#) - [Aerospace Cybersecurity Student Research Spotlight: ERAU](#) - Sean McConoughey, Samuil Nikolov
[Aerospace Village](#) - (12:45-13:30 PDT) - [Aerospace Cybersecurity Student Research Spotlight: Cal Poly](#) - Clara Davis, Dylan Gururajan
[AI Village](#) - cont...(10:00-17:59 PDT) - [Poster Presentations](#) -
[AI Village](#) - cont...(10:00-17:59 PDT) - [Cyber Mirage: Realtime Deepfake Demos](#) - Brandon Kovacs
[AI Village](#) - cont...(10:00-17:59 PDT) - [AI Village: Village Open](#) -
[AppSec Village](#) - cont...(11:30-12:30 PDT) - [Aegis of the Vulnerable: A Unified Pipeline for AI-Based SAST](#) - Can Oztas
[AppSec Village](#) - (12:45-13:45 PDT) - [Drogonsec: SAST + SCA + Secrets + IaC in one open-source scanner](#) - Filipi Pires
[AppSec Village](#) - cont...(10:30-12:30 PDT) - [Burp, But Yours: Hands-On Extension and Bambda Development](#) - Hannah L
[AppSec Village](#) - cont...(11:50-12:20 PDT) - [A Billion-User Blast Radius: Owning ChatGPT's Secure Sandbox](#) - Simcha Kosman
[AppSec Village](#) - (12:30-12:59 PDT) - [Container Escapes Are Not Magic. Here Is How They Actually Work.](#) - Advait Patel
[AppSec Village](#) - cont...(11:00-12:59 PDT) - [Cards Against Vulnerabilities](#) - Patrick Smyth
[AppSec Village](#) - cont...(11:00-12:59 PDT) - [The Call Stack Experience](#) - Victoria Keeler
[AppSec Village](#) - cont...(11:00-12:59 PDT) - [Clash of Prompts: The World's First Prompt Battle Royale](#) -
[AppSec Village](#) - cont...(11:00-12:59 PDT) - [Hack the Duck Store](#) - Gwendal Mognier, Samantha Pearlstein
[Biohacking Village](#) - cont...(10:00-17:59 PDT) - [Embedded & Shredded: Advanced Embedded System Hacking](#) -
[Biohacking Village](#) - cont...(10:00-17:59 PDT) - [Biohacking Device Lab](#) -
[Blacks In Cyber Village](#) - [When the Agent Lies: Why Neurosymbolic AI is the Security Layer Nobody is Building Yet](#) - Maureese Williams
[Blacks In Cyber Village](#) - (12:30-12:55 PDT) - [Prompt Injection Detection in Large Language Models: Survey and Evaluation of Open Source Tools](#) - Yasmin Eady
[Blue Team Village](#) - [Digital Forensics 101](#) - Sarthak Taneja
[Bug Bounty Village](#) - [Write Once, Shell Everywhere: Turning Arbitrary File Writes into RCE](#) - Bruno Mendes, Rafael Castilho Silva
[Bug Bounty Village](#) - (12:30-12:59 PDT) - [Beyond Theoretical Risk: How Cache Poisoning Escalated to Critical Account Takeover in TikTok's Web Infrastructure](#) - Glendon Chong
[Bug Bounty Village](#) - cont...(11:30-12:30 PDT) - [Hackbots](#) - Jason "jhaddix" Haddix, Ryan "BadAt_Computers" Bonner
[Bug Bounty Village](#) - (12:30-13:30 PDT) - [AI Hacking Workshop: Bug Bounty Edition](#) - Ben "NahamSec"
[Sadeghipour, Kameron "clovismint" Bettridge](#)
[Call Center Village](#) - cont...(10:00-17:59 PDT) - [Call Center Village - Open](#) -
[Car Hacking Village](#) - cont...(10:00-16:59 PDT) - [Bomb Bot Challenge](#) -

[Car Hacking Village](#) - cont...(10:00-17:59 PDT) - [Car Hacking Village Open](#) -
[Cloud Village](#) - cont...(11:00-12:59 PDT) - [Weaponizing CloudFormation: Privilege Escalation via Infrastructure as Code in AWS](#) - Samanta Aranda
[Cloud Village](#) - cont...(11:00-12:59 PDT) - [Governing the Firehose: Writing Custom OPA Policies to Tame and Remediate Prowler Output](#) - Ram "n2r"
[Cloud Village](#) - cont...(11:30-12:10 PDT) - [From Pipeline to Cloud Control](#) - Saksham Agrawal
[Cloud Village](#) - [Security at Machine Speed: How Autonomous AI Agents Are Changing Cloud Defense](#) - Pujita Sahni,Geoff Sweet
[Cloud Village](#) - (12:50-13:20 PDT) - [PurpleLoop: Closing the Loop Between Detection Rules, Log Schemas, and Purple-Team Validation](#) - Ariz Soriano
[CodeBloom](#) - [Game Time: Input, Output, and Variables](#) -
[Contests](#) - cont...(10:00-12:59 PDT) - [Aw, man...pages!](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [5N4CK3Y](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [DC's Next Top Threat Model](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Untechnical](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [DEF CON Scavenger Hunt](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Darknet-NG](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Crack Me If You Can 2026](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [TeleChallenge](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [HackFortress](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [?Cube](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [\\$unLight Sh4d0w5](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Octopus Game - Booth Open](#) -
[Contests](#) - cont...(10:00-12:59 PDT) - [Octopus Game Opens and Pre-registration Check-In Available](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Beer Chilling Contraption Contest](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Cryptid Hunt](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [HSPACE: AI Battlegrounds](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [spyVspy 3: Rat Race](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Hacker Games](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [PhreakMe](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Game Hacking Village CTF](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Kubernetes CTF](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Hac-Man](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Crack the Core](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Cyber Deck Competition](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Pinball High Score Contest](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Code Cadaver: Break Every System. Save Your Friend.](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [PWN UR H0M3 - DDoS CTF](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Real7y Overrun - Contest running](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Tin Foil Hat Contest](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [CMD+CTRL Cyber Range: DarkMoney](#) -
[Contests](#) - cont...(11:00-17:59 PDT) - [Radio Frequency Capture the Flag](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [DEF CON CTF: Benevolent Bureau of Birds](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [AI Village Plays Pokemon: DEFCON Edition](#) - Nick Ashworth
[Contests](#) - cont...(10:00-17:59 PDT) - [AI Village - Hal CTF](#) -
[Contests](#) - cont...(10:00-16:59 PDT) - [Car Hacking Village CTF](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [OWASP CTF](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Escalation Desk CTF](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [DEF CON Groups Sticker Contest](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [DEF CON Groups Backdoors & Breaches](#) - Tim Doerges,Seth Benning
[Contests](#) - cont...(10:00-23:59 PDT) - [Apex Park \(Cloud Village CTF\)](#) -
[Contests](#) - [BIC Village Capture the Flag \(CTF\)](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Hacking GRC Contest](#) -
[Contests](#) - [The EFF Benefit Poker Tournament](#) - Cindy Cohn,Jennifer Granick,Marcia Hofmann,Kurt Opsahl,Liz Wharton
[Data Duplication Village](#) - cont...(10:00-17:59 PDT) - [DDV open and accepting drives for duplication](#) -

DCNextGen - Cryptographer Recruitment: Crack the Substitution Cipher - Bradán Lane

DEF CON Groups - cont...(10:00-17:59 PDT) - DEF CON Groups (DCG) -

DEF CON Talks - Your Packets Are Showing: Hybrid Quantum ML for Passive OS Fingerprinting - Daniel Justice,Jae Sung Kim,La Alsulaim,Shreya G Savadatti

DEF CON Talks - (12:30-13:30 PDT) - Fireside Chat with Gen. Paul Nakasone - Paul Nakasone,Jeff "The Dark Tangent" Moss

DEF CON Talks - cont...(11:30-12:30 PDT) - Crashing the Party: Pwning Control-Flow Integrity with Segmentation Fault-Oriented Programming - Marcos "h3xduck" Bajo,Ritvik "RoYalGamr" Goyal

DEF CON Talks - (12:30-13:30 PDT) - BTR Reforged: Weaponizing Defender's Remediation Driver as a Kernel Operation Primitive - Jiří Vinopal

DEF CON Talks - (12:30-12:59 PDT) - DC101 - Nikita Kronenberg,Michael "sparky" Moore,polybius

DEF CON Talks - Shopping Is The Attack: A Decade Of E-Commerce Scalper Wars, And The Multi-Agent AI Era - Yaniv "PSYMAG" Menasherov

DEF CON Talks - (12:30-12:59 PDT) - Hacking the Government: How Two Researchers Turned Late-Night Boredom Into a National Audit - Robert "ProXy" Kruczek,Kamil Szczurowski

DEF CON Talks - cont...(11:30-12:30 PDT) - A Provider for the MOFia - Distributed Post-Ex Capabilities - Steven Flores

DEF CON Talks - (12:30-13:30 PDT) - Patch Gap to Mobile Renderer RCE: Pwning Samsung Internet's V8 on the Galaxy S25 - Hrvoje Mišetić,Jamie Hill-Daniel,William Liu

DEF CON Talks - Can AI do novel security research? Meet the HTTP Terminator - James "albinowax" Kettle

DEF CON Training - cont...(08:30-17:30 PDT) - Beat the Breach: Defend, Respond, Survive - McKay Hardy,Wes Wagstaff

DEF CON Training - cont...(08:30-17:30 PDT) - Cyber & AI Policy Basics: What Every Organization Needs in Place - Pamela 'Pam' Feld,Greg Goldberg

DEF CON Training - cont...(08:30-17:30 PDT) - Digital Supply Chain Security: Software, Cryptography, AI, and Vendor Risk - Anant Shrivastava,Sunil Yadav

DEF CON Workshops - cont...(09:00-12:59 PDT) - Sold Out - Offensive Packet Wizardry with Scapy - Mike "Chicolinux" Guirao

DEF CON Workshops - cont...(09:00-12:59 PDT) - Sold Out - Hands-on IoT firmware extraction and flash forensics - Dennis Giese,Braelynn Luedtke,Arnold Wey,Harsha Potu

DEF CON Workshops - cont...(09:00-12:59 PDT) - Sold Out - AWS Cloud Security 101: From IAM Misconfigurations to Account Takeover - zeta,Rafa "bane" Gutierrez

DEF CON Workshops - cont...(09:00-12:59 PDT) - Sold Out - Web Hacking 101 - cale "calebot" smith,Ruchik Dave,Young Seuk Kim,Luke Cycon

DEF CON Workshops - cont...(09:00-12:59 PDT) - Sold Out - Malware Development 101 - From Zero to Hero: Adapt your payload to your environment - Yoann "OtterHacker" DEQUEKER

DEF CON Workshops - cont...(09:00-12:59 PDT) - Sold Out - Long Live Empire: A C2 Workshop for Modern Red Teaming - Jake "Hubbl3" Krasnov,Vincent "Vinnybod" Rose,Anthony "Coin" Rose,Dan Niefeld

DEF CON Workshops - cont...(09:00-12:59 PDT) - Sold Out - Learning to Hack Bluetooth Low Energy with BLE CTF - Ryan "Hackgnar" Holean,Alek Amrani

DEF CON Workshops - cont...(09:00-12:59 PDT) - Sold Out - Agentic Threat Hunting: Building AI That Remembers What You Hunted - Sydney "letswastetime" Marrone

Demo Labs - Damn Vulnerable Agentic AI Application (DVAIA) - Abhinav Verma,Mukesh Aggarwal

Demo Labs - GnowLab: Open-Source AWS Attack Scenarios Based on Real-World Breaches - ialleejy,Kyul,HyunJun "Beaver King" Kwon

Demo Labs - VoiceLock: Offline, Robust On-Device Speech Transcription - Ayaan Qayyum,Parag Kalay

Demo Labs - Ghost in the IDE - Venkata Jayaram Yalla,Pardhiv Reddy

Demo Labs - Weaponizing eBPF and XDP with Covert Triggered Reverse Shells - Yll "0xBabar0ka" Berisha

Demo Labs - Overcast: Video OSINT Agent. Point It at 100 Videos, Ask Anything - Kevin "kdrwins" Dela Rosa

Embedded Systems Village - cont...(10:00-17:59 PDT) - Exploit Bluetooth Low Energy with BLESPlloit and optional ESP32 - Slawomir Jasek

Embedded Systems Village - cont...(10:00-17:59 PDT) - Embedded - 101 Labs -

Embedded Systems Village - cont...(10:00-17:59 PDT) - Embedded Systems Village CTF -

Game Hacking Village - cont...(10:00-15:59 PDT) - Chill Zone: Casual Games & TASBot Smash Demo -

Game Hacking Village - Riot Games Vanguard: Pwn to own -

Ham Radio Village - Getting Started In Radio Direction Finding - Nate Moore

ICS Village - Threat Hunting in OT Networks - Using Hypothesis Based Methods - Michael Cardwell

IoT Village - cont...(10:00-17:59 PDT) - [Expose Hidden Surveillance in Everyday Tech](#) -

IoT Village - cont...(10:00-17:59 PDT) - [Smart Home in the Matter: Blink, Race, Attack CTF](#) -

IoT Village - cont...(10:00-17:59 PDT) - [Discover GE Appliances!](#) -

IoT Village - cont...(10:00-17:59 PDT) - [Cat-astrophic Hacking: Breaking Into Smart Litter Boxes](#) -

IoT Village - cont...(10:00-17:59 PDT) - [Raiders of the Lost Firmware: A Hands-On Workshop in IoT Firmware Archaeology](#) -

IoT Village - cont...(10:00-17:59 PDT) - [Hands-On Hardware Hacking – From JTAG to Root, Memory Patching Boot Process for Root Access](#) -

IoT Village - cont...(10:00-17:59 PDT) - [All About UART](#) -

IoT Village - cont...(10:00-17:59 PDT) - [Just Hacking Training](#) -

IoT Village - [Build Your Own Meshtastic Node: Off-Grid, Encrypted LoRa Meshnets for Beginners!](#) - Kody Kinzie

IoT Village - (12:30-13:15 PDT) - [Dr. StrangePwn: How I Learned to Stop Worrying and Love the LLM](#) - Larry Pesce

La Villa Community - cont...(11:30-12:30 PDT) - [Demodus Operandi \(Cómo tres rf-hacks en tres bandas terminaron siendo una metodología\)](#) - Eduardo Contreras

La Villa Community - (12:30-12:59 PDT) - [O Lado Sombrio das Coisas: Transformando Dispositivos DIY em Vetores de Ataque](#) - Christiane Borges Santos

La Villa Community - cont...(10:30-12:59 PDT) - [De la nube a la corona: Uso indebido de la identidad híbrida en Azure DevOps Azure, AD, AWS y EKS](#) - Juan Camilo Palacio Arango, Andrés Restrepo

Lonely Hackers Club - cont...(10:00-17:59 PDT) - [Lonely Hackers Club - Lockpicking Table](#) -

Lonely Hackers Club - cont...(10:00-17:59 PDT) - [Lonely Hackers Club - Sticker Swap Table](#) -

Lonely Hackers Club - cont...(10:00-17:59 PDT) - [Lonely Hackers Club CTF](#) -

Lonely Hackers Club - cont...(10:30-16:30 PDT) - [Resume Review with the Lonely Hackers Club](#) -

Maker's Village - cont...(10:00-17:59 PDT) - [Makers' Village - Hacker Arts and Crafts](#) -

Maker's Village - cont...(11:00-12:30 PDT) - [Build-A-Badge Workshop](#) - hunny, Teazee, Buddha, MLP, M-Nelly, Alchemmer

Maker's Village - [Hardhat How-to](#) - m0nkeydrag0n, MrBill

Malware Village - (12:25-13:05 PDT) - [North Korea's Zoo: Poaching for Gophers, Armadillos and RATs](#) - Mauro Eldritch

Malware Village - [Introduction to Reverse Engineering With Ghidra](#) - Wesley McGrew

Maritime Hacking Village - cont...(11:30-12:15 PDT) - [Building the Humans Behind the Mission: Talent, Readiness, and Cyber Power for America's Armed Services](#) - Dr. Nina Kollars, Dr. Wanda T. Jones-Heath, Anne Marie Schumann

Maritime Hacking Village - (12:15-12:59 PDT) - [Maritime Hacking Village Policy Panel: Shadow Fleets, Cyber Effects, and Plausible Deniability](#) - RADM John Mauger, Michael Sulmeyer

Middle Easterns & Africans in Cyber Security (MEACS) - [Once Upon a Prompt: Fairy Tales That Explain AI Security](#) - Sana Talwar

Misc - [From Disk Image to ATT&CK in One Binary — a Reference Architecture for Modern Incident Response \(in Rust\)](#) - HUI Kwun Tai, Albert (4n6h4x0r)

Misc - [Friendship Bracelets](#) -

Mobile Hacking Community - cont...(10:00-17:59 PDT) - [Mobile Hacking - Informal CTF](#) -

Mobile Hacking Community - cont...(10:00-17:59 PDT) - [Mobile Hacking Community - Open](#) -

Mobile Hacking Community - (12:15-12:45 PDT) - [Offensive Security from Your Pocket](#) - Lukas Stefanko

Noob Community - cont...(10:00-17:59 PDT) - [TCM Security Labs](#) -

Noob Community - cont...(10:00-17:59 PDT) - [Skillbit Labs](#) -

Noob Community - cont...(10:00-17:59 PDT) - [SANS Institute NetWars Labs](#) -

Noob Community - cont...(10:00-17:59 PDT) - [Mentoring and Career Advice](#) -

Noob Community - cont...(10:00-17:59 PDT) - [Hack The Box DC Junior Ranger Program Challenge](#) -

Noob Community - cont...(10:00-17:59 PDT) - [Arcanum Security Labs](#) -

Noob Community - cont...(10:00-17:59 PDT) - [No Stupid Questions](#) -

Noob Community - cont...(10:00-17:59 PDT) - [Kryptsec Labs](#) -

Noob Community - cont...(10:00-13:50 PDT) - [Practical Cybersecurity Skills in an AI-Augmented World: Protecting the AI Trifecta](#) - James Stanger, Stephen Schneider

Noob Community - cont...(11:45-12:45 PDT) - [If I Were Eighteen Again: Career Advice for the AI Era](#) - Keith Hoodlet

OSINT For Good Community - cont...(10:00-17:59 PDT) - [OSINT4Good Community - DC NextGen Content](#) -

OSINT For Good Community - cont...(10:00-17:59 PDT) - [FINDX OSINT Educational Series](#) -

OSINT For Good Community - cont...(11:45-12:15 PDT) - [Welcome to OSINT4Good and Trace Labs](#) - Nataly "someone_somewhere"

OSINT For Good Community - (12:30-13:15 PDT) - [Geolocating Talent: How OSINT CTFs are Building Tomorrow's](#)

[Analysts](#) - Ben "The Cyber Sensei" Crenshaw
[OWASP Foundation](#) - cont...(10:00-17:59 PDT) - [BadVR: Signals Everywhere a collaboration with XR Village](#) - Jad Meouchy,Suzanne Borders
[OWASP Foundation](#) - [OWASP ISTG in Practice: A CTF-Style IoT Hacking & Defending Lab](#) - Piero "p33_p33_" Picasso,Aaron Guzman
[Payment Village](#) - [Skimmers, Shimmers, and You](#) - Aidan Quimby
[Physical Security Village](#) - [Flow Like Water: Experiences from Physical Red Teaming](#) - Michael "v3ga" Aguilar
[Physical Security Village](#) - (12:30-12:59 PDT) - [Introduction to RFID](#) - Ege Feyzioglu,Karen Ng
[Policy @ DEF CON](#) - [Election Security in the Age of AI: Governance, Trust, and the Systems Behind Democracy](#) - Lester Godsey,William Gates,Tim Harper
[Queercon Community](#) - [QueerCon Opening Meet and Greet](#) -
[Radio Frequency Village](#) - cont...(10:00-17:59 PDT) - [Radio Frequency Village Events](#) -
[Radio Frequency Village](#) - cont...(10:30-12:25 PDT) - [RF CTF Kick Off Day 1](#) - RF Hackers
[Radio Frequency Village](#) - (12:30-13:25 PDT) - [Let's BLESFlo.it the world together - introducing a new portable Bluetooth Low Energy security tool](#) - Slawomir Jasek
[Recon Village](#) - cont...(10:00-12:30 PDT) - [Hands-On Supply Chain Recon & Vendor Risk Mapping](#) - Dhiyaneshwaran Balasubramaniam,Aman Rawat
[Recon Village](#) - cont...(10:00-23:59 PDT) - [TrackTheFugitive Contest](#) -
[Recon Village](#) - cont...(10:00-23:59 PDT) - [Live Recon Contest](#) -
[Recon Village](#) - cont...(11:00-16:59 PDT) - [GE\(O\)SINT Contest](#) -
[Recon Village](#) - (12:40-15:10 PDT) - [Threat Actors: Gotta Catch 'Em All](#) - Marcelle Lee,Will Thomas
[Red Team Village](#) - cont...(10:00-17:59 PDT) - [From Kiosk to Domain Compromise: Learning to Walk Up and Take it All](#) - Ezra Woods,Mike Manrod,Spencer Alessi
[Red Team Village](#) - cont...(10:00-17:59 PDT) - [BloodHound Quest](#) - Hugo van den Toorn
[Red Team Village](#) - [Burning Redirectors Before Blue Team Does](#) - Mohamed AbuMuslim,Saad Nasir
[Red Team Village](#) - [From Application Telemetry Exposure to Cross-Service Pivoting and Full Azure Tenant Takeover](#) - Chirag Savla,Raunak "Trouble1" Parmar
[Red Team Village](#) - [Web Hacking Bootcamp](#) - Emma Latuszek
[Red Team Village](#) - [Your Passkeys Won't Save You: Conditional Access Bypass via Auth-Method Downgrade](#) - Doug Mooney,Jared Dobbelaer,Jon Rhodes
[Red Team Village](#) - [macOS Doesn't Get Malware...Until It Does](#) - Zoziel Freire
[Red Team Village](#) - [BloodHound OpenGraph Crash Course](#) - JD D
[Scambait Village](#) - cont...(10:00-17:59 PDT) - [Open Q&A](#) -
[Scambait Village](#) - cont...(10:00-17:59 PDT) - [KSCM Scambait Radio](#) -
[Scambait Village](#) - cont...(11:30-13:59 PDT) - [Live Calls Workshop](#) -
[Social Engineering Community Village](#) - cont...(08:30-17:59 PDT) - [Social Engineering Community Village - Open Hours](#) -
[Social Engineering Community Village](#) - [Improv](#) -
[Social Engineering Community Village](#) - [Zero Day Hire: Can You Spot the Spy?](#) - Michael Reimsbach,Rishi "rxerium" C
[Social Gatherings/Events](#) - cont...(08:00-18:59 PDT) - [Human Registration Open](#) -
[Social Gatherings/Events](#) - cont...(10:00-16:59 PDT) - [Malysis: A Bare-Metal RAM Enclave for Malware Analysis. No Hypervisor. No Trace.](#) - Yannick LaRue,Samuel B. G.
[Social Gatherings/Events](#) - cont...(10:00-16:59 PDT) - [Malysis: A Bare-Metal RAM Enclave for Malware Analysis. No Hypervisor. No Trace.](#) - Yannick LaRue,Samuel B. G.
[Social Gatherings/Events](#) - cont...(08:00-17:59 PDT) - [Merch \(formerly swag\) Area Open -- README](#) -
[Social Gatherings/Events](#) - cont...(10:00-18:59 PDT) - [Music](#) - SomaFM -
[Social Gatherings/Events](#) - [Friends of Bill W](#) -
[Telecom Village](#) - cont...(11:00-12:30 PDT) - [SOC Threat Hunting in Practice](#) - Akib Sayyed
[Telecom Village](#) - (12:30-13:15 PDT) - [Poor Man's Mythos: Signal Siege: Agentic Exploit Chains Across the 5G Cloud-Native Stack](#) - Omer Farooq
[The Diana Initiative](#) - [DEF CON Academy Tour](#) -
[The Diana Initiative](#) - [DC Maker's Community Tour](#) -
[The Diana Initiative](#) - (12:20-12:30 PDT) - [Cryptocurrency Village Tour](#) -
[The Diana Initiative](#) - (12:30-12:40 PDT) - [Car Hacking Village Tour](#) -
[The Diana Initiative](#) - (12:40-12:50 PDT) - [Call Center Tour](#) -
[The Diana Initiative](#) - (12:50-12:59 PDT) - [DDoS Community Tour](#) -

[The Diana Initiative](#) - [The Diana Initiative](#) - [Open time](#) -
[Voting Village](#) - [cont...\(10:00-17:59 PDT\)](#) - [Voting Village Lab](#) -
[Voting Village](#) - [Voting Village Keynote](#) - [The Paper Chase](#) - [Kevin Shelley](#)

[.EDU Community](#) - [ScamBusters: Turning Undergrads into Threat Hunters](#) - Angela "BlondeTechie" Ramos
[Adversary Village](#) - (13:15-13:59 PDT) - [From threat-intel to tested defense, the adversary simulation playbook](#) - Cheryl Biswas,Adam Pennington,Olaf Hartong,Sarah Hume
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Mission: Compromised - Hacking a Satellite from the Ground Up](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [MOUSE Runner & Flappy Drone](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Flight Simulator/EFB](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Drone Hacking Workshop](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Nebula Showdown: Space Systems Security CTF Adventure](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [SR-71 Blackbird Badge Challenge](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Satellites Under Attack: Hands-On Satellite Security Threat Scenarios](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [SpaceCOP - Catch Me If You Can](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [ARINC 664 CTF Challenge](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Aerospace Ecosystem Resilience Innovation Environment \(AERIE\) Cyber Range](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Aviation ISAC Cybersecurity Challenge](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Drone Hacking Choose your Own Adventure](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [DCNextGen - Space Grand Challenge - SatHack: The MOUSE-1 Mission](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [DCNextGen - RIC-1: ELT Localization Exercise - N3VR-G0N Down](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [DCNextGen - Bricks in the Air](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Bricks in the Air](#) -
[Aerospace Village](#) - cont...(12:45-13:30 PDT) - [Aerospace Cybersecurity Student Research Spotlight: Cal Poly](#) - Clara Davis,Dylan Gururajan
[Aerospace Village](#) - (13:30-13:59 PDT) - [Hacking Airplanes at the NTSB](#) - David Case,Jonathan Xue
[AI Village](#) - cont...(10:00-17:59 PDT) - [Cyber Mirage: Realtime Deepfake Demos](#) - Brandon Kovacs
[AI Village](#) - cont...(10:00-17:59 PDT) - [Poster Presentations](#) -
[AI Village](#) - cont...(10:00-17:59 PDT) - [AI Village: Village Open](#) -
[AppSec Village](#) - cont...(12:45-13:45 PDT) - [Drogonsec: SAST + SCA + Secrets + IaC in one open-source scanner](#) - Filippires
[AppSec Village](#) - (13:30-13:59 PDT) - [Agentic Chaos - What 86K+ Agent Codebases Reveal About 700K+ Exposed AI Systems](#) - Bar Kaduri,Lidan
[AppSec Village](#) - [Cards Against Vulnerabilities](#) - Patrick Smyth
[AppSec Village](#) - [AI Pentesting Trivia Showdown](#) - Andy Dennis,Bill Reyor
[AppSec Village](#) - [Factory Floor MVP Incident Response Challenge](#) -
[AppSec Village](#) - [AppSec Quiz Gauntlet: Spot the Vulnerability](#) - Avek Kolech
[Biohacking Village](#) - cont...(10:00-17:59 PDT) - [Embedded & Shredded: Advanced Embedded System Hacking](#) -
[Biohacking Village](#) - cont...(10:00-17:59 PDT) - [Biohacking Device Lab](#) -
[Blacks In Cyber Village](#) - [CTRL the Chaos: When AI Controls Critical Infrastructure](#) - Nykolas Muldrow
[Blue Team Village](#) - (13:15-14:15 PDT) - [TBA](#) -
[Bug Bounty Village](#) - cont...(12:30-13:30 PDT) - [AI Hacking Workshop: Bug Bounty Edition](#) - Ben "NahamSec" Sadeghipour,Kameron "clovismint" Bettridge
[Call Center Village](#) - cont...(10:00-17:59 PDT) - [Call Center Village - Open](#) -
[Car Hacking Village](#) - cont...(10:00-17:59 PDT) - [Car Hacking Village Open](#) -
[Car Hacking Village](#) - cont...(10:00-16:59 PDT) - [Bomb Bot Challenge](#) -
[Cloud Village](#) - (13:30-15:30 PDT) - [Cloudy with a Chance of Breaches: Hands-On AWS Threat Defense](#) - Kyle Hubbard
[Cloud Village](#) - (13:30-14:30 PDT) - [The Autonomous Security Loop](#) - Jeremy Schiefer,Lawton Pittenger
[Cloud Village](#) - cont...(12:50-13:20 PDT) - [PurpleLoop: Closing the Loop Between Detection Rules, Log Schemas, and Purple-Team Validation](#) - Ariz Soriano
[Cloud Village](#) - (13:20-13:59 PDT) - [The Hidden Cost of Agentic Connectivity](#) - David Fiser,Amy McMahon
[CodeBloom](#) - [What is AI?](#) - Sam Mosley
[Contests](#) - cont...(10:00-17:59 PDT) - [5N4CK3Y](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [DC's Next Top Threat Model](#) -

[Contests](#) - cont...(10:00-17:59 PDT) - [Untechnical](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [DEF CON Scavenger Hunt](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Darknet-NG](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Crack Me If You Can 2026](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [TeleChallenge](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [HackFortress](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [?Cube](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [\\$unLight Sh4d0w5](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Octopus Game - Booth Open](#) -
[Contests](#) - [Octopus Game - Walk-In Registration \(Pre-Registration Check-In Closed\)](#) -
[Contests](#) - (13:30-14:59 PDT) - [Octopus Game - Booth Battle #1: The Front Man's Wager](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Beer Chilling Contraption Contest](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Cryptid Hunt](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [HSPACE: AI Battlegrounds](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [spyVspy 3: Rat Race](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Hacker Games](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [PhreakMe](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Game Hacking Village CTF](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Kubernetes CTF](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Hac-Man](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Crack the Core](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Cyber Deck Competition](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Pinball High Score Contest](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Code Cadaver: Break Every System. Save Your Friend.](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [PWN UR H0M3 - DDoS CTF](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Real7y Overrun - Contest running](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Tin Foil Hat Contest](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [CMD+CTRL Cyber Range: DarkMoney](#) -
[Contests](#) - [Locktopus - Open Qualifying](#) -
[Contests](#) - cont...(11:00-17:59 PDT) - [Radio Frequency Capture the Flag](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [DEF CON CTF: Benevolent Bureau of Birds](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [AI Village - Hal CTF](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [AI Village Plays Pokemon: DEFCON Edition](#) - Nick Ashworth
[Contests](#) - cont...(10:00-16:59 PDT) - [Car Hacking Village CTF](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [OWASP CTF](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Escalation Desk CTF](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [DEF CON Groups Sticker Contest](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [DEF CON Groups Backdoors & Breaches](#) - Tim Doerges,Seth Benning
[Contests](#) - cont...(10:00-23:59 PDT) - [Apex Park \(Cloud Village CTF\)](#) -
[Contests](#) - [SEC Vishing Competition \(SECVC\)](#) -
[Contests](#) - [Pub Quiz at DEF CON](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Hacking GRC Contest](#) -
[Contests](#) - cont...(12:00-14:59 PDT) - [The EFF Benefit Poker Tournament](#) - Cindy Cohn,Jennifer Granick,Marcia Hofmann,Kurt Opsahl,Liz Wharton
[Crypto & Privacy Village](#) - [Trust the Basics, But Know Their Limits: Where Standard Cybersecurity Advice Falls Short](#) - Yael Grauer
[Data Duplication Village](#) - cont...(10:00-17:59 PDT) - [DDV open and accepting drives for duplication](#) -
[Data Duplication Village](#) - [Forcing Physical Interlocks into Data Transit and Storage Replication](#) - Mehmet Önder Key,Temel Demir
[DCNextGen](#) - [Locked Out? Let's Fix That: An Introduction to the Art of Lockpicking](#) - Greg Anderson
[DEF CON Groups](#) - cont...(10:00-17:59 PDT) - [DEF CON Groups \(DCG\)](#) -
[DEF CON Groups](#) - (13:30-14:30 PDT) - [Darknet Diaries Meet & Greet with Jack Rhysider](#) - Jack Rhysider
[DEF CON Talks](#) - cont...(12:30-13:30 PDT) - [Fireside Chat with Gen. Paul Nakasone](#) - Paul Nakasone,Jeff "The Dark Tangent" Moss
[DEF CON Talks](#) - (13:30-14:59 PDT) - [What is the Right Balance of Rules for Defenders & Adversaries? Determining which](#)

dual-use model restrictions make sense and which only disarm defenders - Emanuel Gawrieh,Jason Clinton,Bruce Schneider,Heather Adkins

DEF CON Talks - cont...(12:30-13:30 PDT) - BTR Reforged: Weaponizing Defender's Remediation Driver as a Kernel Operation Primitive - Jiří Vinopal

DEF CON Talks - (13:30-14:30 PDT) - Breaking into Amazon lockers by any means necessary - Martin Vigo

DEF CON Talks - LGTM: Bypassing an LLM Build Gate When Prompt Injection Fails - Aviv Donenfeld

DEF CON Talks - cont...(12:30-13:30 PDT) - Patch Gap to Mobile Renderer RCE: Pwning Samsung Internet's V8 on the Galaxy S25 - Hrvoje Mišetić,Jamie Hill-Daniel,William Liu

DEF CON Talks - (13:30-14:30 PDT) - Plug And Pwn: Weaponizing Windows PnP Auto-Install - Alejandro "0xedh" Hernandez,Borja "borjnz" Martinez

DEF CON Talks - Bring-Your-Own-EDR - Breaking Windows Process Protection to build EDR-Protected Malware - Shahak Morag

DEF CON Training - cont...(08:30-17:30 PDT) - Beat the Breach: Defend, Respond, Survive - McKay Hardy,Wes Wagstaff

DEF CON Training - cont...(08:30-17:30 PDT) - Cyber & AI Policy Basics: What Every Organization Needs in Place - Pamela 'Pam' Feld,Greg Goldberg

DEF CON Training - cont...(08:30-17:30 PDT) - Digital Supply Chain Security: Software, Cryptography, AI, and Vendor Risk - Anant Shrivastava,Sunil Yadav

Demo Labs - xEndity: IoT Firmware Analysis & Digital Twin Platform - Zeus "LightningGod" Chan,Kenneth "kenleejl" Lee

Demo Labs - MSCodePhish: Redeem Your Coupon. Surrender Your Session - Raunak "Trouble1" Parmar,Chirag "3xpl01tc0d3r" Savla

Demo Labs - Goose Processing Unit (GPU): VRAM as an Unmonitored Attack Surface - Gannon "Dorf" Gebauer,Anthony "Coin" Rose,Hana Christensen

Demo Labs - Zero-Cloud Threat Modeling: Vector Embedding Architectures for Automated Vulnerability Detection - Ankit Vashisth

Demo Labs - Beyond Spidering: Behavior Driven DAST for Real Application Workflows - Sara "testingSoul" Martinez

Demo Labs - Monitor, Compile, Enforce: A Compiler Pipeline for Container Security Policy in Rust and eBPF - Buğrahan Yücel

Embedded Systems Village - cont...(10:00-17:59 PDT) - Exploit Bluetooth Low Energy with BLESPlloit and optional ESP32 - Slawomir Jasek

Embedded Systems Village - cont...(10:00-17:59 PDT) - Embedded - 101 Labs -

Embedded Systems Village - cont...(10:00-17:59 PDT) - Embedded Systems Village CTF -

Game Hacking Village - cont...(10:00-15:59 PDT) - Chill Zone: Casual Games & TASBot Smash Demo -

Game Hacking Village - cont...(12:00-16:59 PDT) - Riot Games Vanguard: Pwn to own -

Hackers.town - The Cum-Stained Precipice of Digital Redlining - Erica Rachel Andrews,Abbie Gonzalez (pronounced AB)

Hackers.town - Liberate your Music with Tech Reclaimers - RemoteNemesis

Ham Radio Village - Ham Radio Isn't Magic: Preppers, Sad Hams, and Practical Off-Grid Communications - Andrew Ohnstad - N3OCQ

IoT Village - cont...(10:00-17:59 PDT) - All About UART -

IoT Village - cont...(10:00-17:59 PDT) - Discover GE Appliances! -

IoT Village - cont...(10:00-17:59 PDT) - Cat-astrophic Hacking: Breaking Into Smart Litter Boxes -

IoT Village - cont...(10:00-17:59 PDT) - Raiders of the Lost Firmware: A Hands-On Workshop in IoT Firmware Archaeology -

IoT Village - cont...(10:00-17:59 PDT) - Hands-On Hardware Hacking – From JTAG to Root, Memory Patching Boot Process for Root Access -

IoT Village - cont...(10:00-17:59 PDT) - Just Hacking Training -

IoT Village - cont...(10:00-17:59 PDT) - Expose Hidden Surveillance in Everyday Tech -

IoT Village - cont...(10:00-17:59 PDT) - Smart Home in the Matter: Blink, Race, Attack CTF -

IoT Village - cont...(12:00-13:30 PDT) - Build Your Own Meshtastic Node: Off-Grid, Encrypted LoRa Meshnets for Beginners! - Kody Kinzie

IoT Village - (13:45-15:15 PDT) - Mesh Nets for Hackers: How (& When) to use Meshtastic, Meshcore, & Reticulum! - Kody Kinzie

IoT Village - cont...(12:30-13:15 PDT) - Dr. Strangepwn: How I Learned to Stop Worrying and Love the LLM - Larry Pesce

La Villa Community - AImaru C2: La Nueva Era del Living off the Land (MCP AI-Driven C2) - Mario Lobo

Lockpick Village - Intro to Lockpicking -

Lonely Hackers Club - cont...(10:00-17:59 PDT) - Lonely Hackers Club - Sticker Swap Table -

[Lonely Hackers Club](#) - cont...(10:00-17:59 PDT) - [Lonely Hackers Club CTF](#) -
[Lonely Hackers Club](#) - cont...(10:00-17:59 PDT) - [Lonely Hackers Club - Lockpicking Table](#) -
[Lonely Hackers Club](#) - cont...(10:30-16:30 PDT) - [Resume Review with the Lonely Hackers Club](#) -
[Maker's Village](#) - cont...(10:00-17:59 PDT) - [Makers' Village - Hacker Arts and Crafts](#) -
[Malware Village](#) - cont...(12:25-13:05 PDT) - [North Korea's Zoo: Poaching for Gophers, Armadillos and RATs](#) - Mauro Eldritch
[Malware Village](#) - (13:15-13:55 PDT) - [Return of Sedinho: Current situation and new tactics of the Brazilian banking trojan ecosystem](#) - Josep Albors
[Malware Village](#) - cont...(12:10-14:10 PDT) - [Introduction to Reverse Engineering With Ghidra](#) - Wesley McGrew
[Maritime Hacking Village](#) - (13:45-14:15 PDT) - [Drag, Drop, Deploy, Compromise: Why Trusted HMI Engineering Toolchains Remain an ICS Supply-Chain Blind Spot](#) - Jiwoon Yoo,TaeWoo Kim,Eunji choi
[Middle Easterns & Africans in Cyber Security \(MEACS\)](#) - [Nothing Wrong Here: Why AI Artifact Scanners Wave Malware Through](#) - Amber Bennoui
[Mobile Hacking Community](#) - cont...(10:00-17:59 PDT) - [Mobile Hacking Community - Open](#) -
[Mobile Hacking Community](#) - cont...(10:00-17:59 PDT) - [Mobile Hacking - Informal CTF](#) -
[Mobile Hacking Community](#) - [Hacking Android Apps in a Structured Way](#) - Sven Schleier
[Nix Vegas Community](#) - [Whose PR Is It Anyway?](#) -
[Noob Community](#) - cont...(10:00-17:59 PDT) - [TCM Security Labs](#) -
[Noob Community](#) - cont...(10:00-17:59 PDT) - [Skillbit Labs](#) -
[Noob Community](#) - cont...(10:00-17:59 PDT) - [SANS Institute NetWars Labs](#) -
[Noob Community](#) - cont...(10:00-17:59 PDT) - [Hack The Box DC Junior Ranger Program Challenge](#) -
[Noob Community](#) - cont...(10:00-17:59 PDT) - [Mentoring and Career Advice](#) -
[Noob Community](#) - cont...(10:00-17:59 PDT) - [No Stupid Questions](#) -
[Noob Community](#) - cont...(10:00-17:59 PDT) - [Arcanum Security Labs](#) -
[Noob Community](#) - cont...(10:00-17:59 PDT) - [Kryptsec Labs](#) -
[Noob Community](#) - cont...(10:00-13:50 PDT) - [Practical Cybersecurity Skills in an AI-Augmented World: Protecting the AI Trifecta](#) - James Stanger,Stephen Schneiter
[Noob Community](#) - [Threatmaxxing Your Stakeholders while Mogging Your Threat Actors: What is Cyber Threat Intel?](#) - Eli Woodward
[Noob Community](#) - (13:30-13:59 PDT) - [OSINT: Zero To Hero](#) - Mishaal Khan
[OSINT For Good Community](#) - (13:30-14:30 PDT) - [Classical OSINT using AI \(Actual Intelligence\)](#) - Bianca C. Ionescu/reconcerto
[OSINT For Good Community](#) - cont...(10:00-17:59 PDT) - [OSINT4Good Community - DC NextGen Content](#) -
[OSINT For Good Community](#) - cont...(10:00-17:59 PDT) - [FINDX OSINT Educational Series](#) -
[OSINT For Good Community](#) - cont...(12:30-13:15 PDT) - [Geolocating Talent: How OSINT CTFs are Building Tomorrow's Analysts](#) - Ben "The Cyber Sensei" Crenshaw
[OWASP Foundation](#) - cont...(10:00-17:59 PDT) - [BadVR: Signals Everywhere a collaboration with XR Village](#) - Jad Meouchy,Suzanne Borders
[OWASP Foundation](#) - cont...(12:00-13:59 PDT) - [OWASP ISTG in Practice: A CTF-Style IoT Hacking & Defending Lab](#) - Piero "p33_p33_" Picasso,Aaron Guzman
[Payment Village](#) - (13:30-13:59 PDT) - [It's a Payment Terminal. It's My Arcade. It's Everywhere. It Cost Me Nine Bucks.](#) - Chiao-Lin Yu "Steven Meow"
[Payment Village](#) - [Wall of Wallets Workshop \(Intro to Wall of Wallets Challenge\)](#) - Dan Borgogno
[Policy @ DEF CON](#) - [Connectivity as Control in the European High North](#) - Szymon Skalski,Patricia Vargas Leon,Jorge Acevedo Canabal
[Policy @ DEF CON](#) - [The Cyber Crystal Ball: The Annual Policy @ DEF CON Contingencies Survey](#) - Matthew Wein,Bruce Schneier,Chris Painter,Heather West
[Queercon Community](#) - [Non-Binary/Gender Non-conforming Meetup](#) -
[Radio Frequency Village](#) - cont...(10:00-17:59 PDT) - [Radio Frequency Village Events](#) -
[Radio Frequency Village](#) - cont...(12:30-13:25 PDT) - [Let's BLESPl0.it the world together - introducing a new portable Bluetooth Low Energy security tool](#) - Slawomir Jasek
[Radio Frequency Village](#) - (13:30-14:25 PDT) - [Fox Hunting - Finding Rogue Access Points in the CTF and in the Wild](#) - Eric Escobar
[Radio Frequency Village](#) - [Running your own LTE network for fun and profit????](#) - Lozaning
[Recon Village](#) - cont...(10:00-23:59 PDT) - [TrackTheFugitive Contest](#) -

[Recon Village - cont...\(10:00-23:59 PDT\) - Live Recon Contest -](#)
[Recon Village - cont...\(11:00-16:59 PDT\) - GE\(O\)SINT Contest -](#)
[Recon Village - cont...\(12:40-15:10 PDT\) - Threat Actors: Gotta Catch 'Em All - Marcelle Lee,Will Thomas](#)
[Recon Village - OSINT Is Still a Thinking Game: Surviving AI Without Losing Tradecraft - Nico Dekens](#)
[Red Team Village - cont...\(10:00-17:59 PDT\) - From Kiosk to Domain Compromise: Learning to Walk Up and Take it All - Ezra Woods, Mike Manrod, Spencer Alessi](#)
[Red Team Village - cont...\(10:00-17:59 PDT\) - BloodHound Quest - Hugo van den Toorn](#)
[Red Team Village - cont...\(12:00-13:59 PDT\) - Burning Redirectors Before Blue Team Does - Mohamed AbuMuslim, Saad Nasir](#)
[Red Team Village - cont...\(12:00-13:59 PDT\) - From Application Telemetry Exposure to Cross-Service Pivoting and Full Azure Tenant Takeover - Chirag Savla, Raunak "Trouble1" Parmar](#)
[Red Team Village - cont...\(12:00-13:59 PDT\) - Web Hacking Bootcamp - Emma Latuszek](#)
[Red Team Village - cont...\(12:00-13:59 PDT\) - Your Passkeys Won't Save You: Conditional Access Bypass via Auth-Method Downgrade - Doug Mooney, Jared Dobbelaer, Jon Rhodes](#)
[Red Team Village - Shapeshifting C2: Applying DAITA Traffic Shaping to Defeat DPI and DLP Detection - Rafael Felix](#)
[Red Team Village - One Request to Rule Them All - Corey Ball](#)
[Red Team Village - BloodHound OpenGraph: Six Degrees of Everything - Rohan Vazarkar, Wes Miller](#)
[Scambait Village - cont...\(10:00-17:59 PDT\) - Open Q&A -](#)
[Scambait Village - cont...\(10:00-17:59 PDT\) - KSCM Scambait Radio -](#)
[Scambait Village - cont...\(11:30-13:59 PDT\) - Live Calls Workshop -](#)
[Social Engineering Community Village - cont...\(08:30-17:59 PDT\) - Social Engineering Community Village - Open Hours -](#)
[Social Engineering Community Village - \(13:30-14:30 PDT\) - Zero Day Hire: Can You Spot the Spy? - Michael Reimsbach, Rishi "rxerium" C](#)
[Social Gatherings/Events - cont...\(08:00-18:59 PDT\) - Human Registration Open -](#)
[Social Gatherings/Events - cont...\(10:00-16:59 PDT\) - Malysis: A Bare-Metal RAM Enclave for Malware Analysis. No Hypervisor. No Trace. - Yannick LaRue, Samuel B. G.](#)
[Social Gatherings/Events - cont...\(10:00-16:59 PDT\) - Malysis: A Bare-Metal RAM Enclave for Malware Analysis. No Hypervisor. No Trace. - Yannick LaRue, Samuel B. G.](#)
[Social Gatherings/Events - Book Signing - Brandy Smith - Brandy Smith](#)
[Social Gatherings/Events - cont...\(08:00-17:59 PDT\) - Merch \(formerly swag\) Area Open -- README -](#)
[Social Gatherings/Events - cont...\(10:00-18:59 PDT\) - Music - SomaFM -](#)
[Social Gatherings/Events - Free Ham Radio License Exams -](#)
[Telecom Village - cont...\(12:30-13:15 PDT\) - Poor Man's Mythos: Signal Siege: Agentic Exploit Chains Across the 5G Cloud-Native Stack - Omer Farooq](#)
[The Diana Initiative - Cloud Village Tour -](#)
[The Diana Initiative - Telecom Village Tour -](#)
[The Diana Initiative - \(13:20-13:30 PDT\) - DEF CON Groups \(DCG\) Tour -](#)
[The Diana Initiative - \(13:30-13:40 PDT\) - Aerospace Village Tour -](#)
[The Diana Initiative - \(13:40-13:50 PDT\) - Bug Bounty Village Tour -](#)
[The Diana Initiative - \(13:50-13:59 PDT\) - La Villa Tour -](#)
[The Diana Initiative - Stigma is stupid: Let's talk about recovery, mental wellness, and hard stuff without making it awkward - Jennifer VanAntwerp](#)
[Voting Village - cont...\(10:00-17:59 PDT\) - Voting Village Lab -](#)
[Voting Village - \(13:30-13:59 PDT\) - Publicly Auditable Elections - Josh Benaloah](#)

[Return to Index](#) - [Locations Legend](#)

[.EDU Community - Hacking Education - Teaching Offensive Cyber Science at the Collegiate Level](#) - Dave "Rebelcadet" Ortiz
[Adversary Village - 6 years of Adversary Village! Keeping up with the adversaries and why it takes a village](#) - Abhijith "Abx" B R, Bryson Bort, Anant Shrivastava
[Adversary Village - \(14:45-15:15 PDT\) - SEND: Teaching Machines to Lie to Defenders](#) - Yi Ting Shen, Ariz Soriano
[Aerospace Village - cont...\(10:00-17:59 PDT\) - Satellites Under Attack: Hands-On Satellite Security Threat Scenarios](#) -
[Aerospace Village - cont...\(10:00-17:59 PDT\) - Nebula Showdown: Space Systems Security CTF Adventure](#) -
[Aerospace Village - cont...\(10:00-17:59 PDT\) - SR-71 Blackbird Badge Challenge](#) -
[Aerospace Village - cont...\(10:00-17:59 PDT\) - SpaceCOP - Catch Me If You Can](#) -
[Aerospace Village - cont...\(10:00-17:59 PDT\) - MOUSE Runner & Flappy Drone](#) -
[Aerospace Village - cont...\(10:00-17:59 PDT\) - Mission: Compromised - Hacking a Satellite from the Ground Up](#) -
[Aerospace Village - cont...\(10:00-17:59 PDT\) - Flight Simulator/EFB](#) -
[Aerospace Village - cont...\(10:00-17:59 PDT\) - Drone Hacking Workshop](#) -
[Aerospace Village - cont...\(10:00-17:59 PDT\) - ARINC 664 CTF Challenge](#) -
[Aerospace Village - cont...\(10:00-17:59 PDT\) - Aerospace Ecosystem Resilience Innovation Environment \(AERIE\) Cyber Range](#) -
[Aerospace Village - cont...\(10:00-17:59 PDT\) - Drone Hacking Choose your Own Adventure](#) -
[Aerospace Village - cont...\(10:00-17:59 PDT\) - Bricks in the Air](#) -
[Aerospace Village - cont...\(10:00-17:59 PDT\) - Aviation ISAC Cybersecurity Challenge](#) -
[Aerospace Village - cont...\(10:00-17:59 PDT\) - DCNextGen - Space Grand Challenge - SatHack: The MOUSE-1 Mission](#) -
[Aerospace Village - cont...\(10:00-17:59 PDT\) - DCNextGen - RIC-1: ELT Localization Exercise - N3VR-G0N Down](#) -
[Aerospace Village - cont...\(10:00-17:59 PDT\) - DCNextGen - Bricks in the Air](#) -
[AI Village - cont...\(10:00-17:59 PDT\) - AI Village: Village Open](#) -
[AI Village - cont...\(10:00-17:59 PDT\) - Poster Presentations](#) -
[AI Village - cont...\(10:00-17:59 PDT\) - Cyber Mirage: Realtime Deepfake Demos](#) - Brandon Kovacs
[AI Village - Fooling Coding Agents for Fun and Profit](#) - Matt Galligan, Jack Cable
[AppSec Village - Farsight: Turning OSINT into Actionable Attack Surface Intelligence](#) - Arif, Sai Vernekar, Seedon D'Souza, kvprashant
[AppSec Village - \(14:30-16:59 PDT\) - Container Escapes 101](#) - some-natalie
[AppSec Village - from_pretrained\(\) to from_pwned\(\): Breaking HuggingFace's Trust](#) - Yotam Perkal
[AppSec Village - \(14:50-15:20 PDT\) - GeoHacking: from memory corruption RCE to cross tenant access](#) - Michal Kamensky
[AppSec Village - cont...\(13:00-14:59 PDT\) - Cards Against Vulnerabilities](#) - Patrick Smyth
[AppSec Village - cont...\(13:00-14:59 PDT\) - AI Pentesting Trivia Showdown](#) - Andy Dennis, Bill Reyor
[AppSec Village - cont...\(13:00-14:59 PDT\) - Factory Floor MVP Incident Response Challenge](#) -
[AppSec Village - cont...\(13:00-14:59 PDT\) - AppSec Quiz Gauntlet: Spot the Vulnerability](#) - Avek Kolech
[Biohacking Village - cont...\(10:00-17:59 PDT\) - Biohacking Device Lab](#) -
[Biohacking Village - cont...\(10:00-17:59 PDT\) - Embedded & Shredded: Advanced Embedded System Hacking](#) -
[Blacks In Cyber Village - Agents on Alert: Building an AI-Powered Threat Investigation Framework](#) - Samson Adewale
[Blue Team Village - cont...\(13:15-14:15 PDT\) - TBA](#) -
[Blue Team Village - \(14:30-15:30 PDT\) - Building Project Obsidian: Designing the Blue Team CTF for DEF CON](#) - Carlo Anez Mazurco, Chris "dafinga" Maenner, Omenscan ~, Paul Goffar
[Bug Bounty Village - AI Nightmare: Hacking at 0-Hour](#) - Pedro "drop" Paniago
[Bug Bounty Village - Navigating AI-Assisted Submissions](#) - Tony Lee, Michael Skelton, Alexander Wren, Selim Jaafar, Shlomie "shlibness" Liberow
[Call Center Village - cont...\(10:00-17:59 PDT\) - Call Center Village - Open](#) -
[Car Hacking Village - cont...\(10:00-16:59 PDT\) - Bomb Bot Challenge](#) -
[Car Hacking Village - cont...\(10:00-17:59 PDT\) - Car Hacking Village Open](#) -
[Cloud Village - cont...\(13:30-15:30 PDT\) - Cloudy with a Chance of Breaches: Hands-On AWS Threat Defense](#) - Kyle Hubbard
[Cloud Village - cont...\(13:30-14:30 PDT\) - The Autonomous Security Loop](#) - Jeremy Schiefer, Lawton Pittenger
[Cloud Village - Nebula - 5 years, still kicking *aaS](#) - Bleon "gl4ssesbo1" Proko
[Cloud Village - \(14:30-15:10 PDT\) - Citizen Developers Can't Defend What They Built: Scaling Security Past the Security](#)

Team -
 CodeBloom - Work Session: Ciphers -
 Contests - DEF CON Beard and Mustache Contest -
 Contests - cont...(10:00-17:59 PDT) - 5N4CK3Y -
 Contests - cont...(10:00-17:59 PDT) - DC's Next Top Threat Model -
 Contests - cont...(10:00-17:59 PDT) - Untechnical -
 Contests - cont...(10:00-17:59 PDT) - DEF CON Scavenger Hunt -
 Contests - cont...(10:00-17:59 PDT) - Darknet-NG -
 Contests - cont...(10:00-17:59 PDT) - Crack Me If You Can 2026 -
 Contests - cont...(10:00-17:59 PDT) - TeleChallenge -
 Contests - cont...(10:00-17:59 PDT) - HackFortress -
 Contests - cont...(10:00-17:59 PDT) - ?Cube -
 Contests - cont...(10:00-17:59 PDT) - \$unLight Sh4d0w5 -
 Contests - cont...(10:00-17:59 PDT) - Octopus Game - Booth Open -
 Contests - cont...(13:30-14:59 PDT) - Octopus Game - Booth Battle #1: The Front Man's Wager -
 Contests - cont...(10:00-17:59 PDT) - Beer Chilling Contraption Contest -
 Contests - cont...(10:00-17:59 PDT) - Cryptid Hunt -
 Contests - cont...(10:00-17:59 PDT) - HSPACE: AI Battlegrounds -
 Contests - cont...(10:00-17:59 PDT) - spyVspy 3: Rat Race -
 Contests - cont...(10:00-17:59 PDT) - Hacker Games -
 Contests - cont...(10:00-17:59 PDT) - PhreakMe -
 Contests - cont...(10:00-17:59 PDT) - Game Hacking Village CTF -
 Contests - cont...(10:00-17:59 PDT) - Kubernetes CTF -
 Contests - cont...(10:00-17:59 PDT) - Hac-Man -
 Contests - cont...(10:00-17:59 PDT) - Crack the Core -
 Contests - cont...(10:00-17:59 PDT) - Cyber Deck Competition -
 Contests - cont...(10:00-17:59 PDT) - Pinball High Score Contest -
 Contests - cont...(10:00-17:59 PDT) - Code Cadaver: Break Every System. Save Your Friend. -
 Contests - cont...(10:00-17:59 PDT) - PWN UR H0M3 - DDoS CTF -
 Contests - cont...(10:00-17:59 PDT) - Real7y Overrun - Contest running -
 Contests - cont...(10:00-17:59 PDT) - Tin Foil Hat Contest -
 Contests - cont...(10:00-17:59 PDT) - CMD+CTRL Cyber Range: DarkMoney -
 Contests - cont...(13:00-17:59 PDT) - Locktopus - Open Qualifying -
 Contests - cont...(11:00-17:59 PDT) - Radio Frequency Capture the Flag -
 Contests - cont...(10:00-17:59 PDT) - DEF CON CTF: Benevolent Bureau of Birds -
 Contests - cont...(10:00-17:59 PDT) - AI Village - Hal CTF -
 Contests - cont...(10:00-17:59 PDT) - AI Village Plays Pokemon: DEFCON Edition - Nick Ashworth
 Contests - cont...(10:00-16:59 PDT) - Car Hacking Village CTF -
 Contests - cont...(10:00-17:59 PDT) - OWASP CTF -
 Contests - cont...(10:00-17:59 PDT) - Escalation Desk CTF -
 Contests - cont...(10:00-17:59 PDT) - DEF CON Groups Backdoors & Breaches - Tim Doerges,Seth Benning
 Contests - cont...(10:00-17:59 PDT) - DEF CON Groups Sticker Contest -
 Contests - cont...(10:00-23:59 PDT) - Apex Park (Cloud Village CTF) -
 Contests - cont...(13:00-15:59 PDT) - SEC Vishing Competition (SECV) -
 Contests - cont...(13:00-14:59 PDT) - Pub Quiz at DEF CON -
 Contests - cont...(10:00-17:59 PDT) - Hacking GRC Contest -
 Contests - cont...(12:00-14:59 PDT) - The EFF Benefit Poker Tournament - Cindy Cohn,Jennifer Granick,Marcia Hofmann,Kurt Opsahl,Liz Wharton
 Crypto & Privacy Village - (14:30-14:59 PDT) - You're Probably Using FPE Wrong - Leslie Gutschow
 Crypto & Privacy Village - Inside the Guts of Ransomware - Ashley Hiram Muñoz
 Cryptocurrency Village - Cryptohack Badge Hacking - Do Truong Giang "FSNaix",Sadiq "Sdqmd",Arjun "Peper" Suresh
 Data Duplication Village - cont...(10:00-17:59 PDT) - DDV open and accepting drives for duplication -
 DCNextGen - Hack the Airwaves – Embedded Wireless for Next-Gen Hackers - Adventures of Illya
 DEF CON Groups - cont...(10:00-17:59 PDT) - DEF CON Groups (DCG) -
 DEF CON Groups - cont...(13:30-14:30 PDT) - Darknet Diaries Meet & Greet with Jack Rhysider - Jack Rhysider

DEF CON Talks - cont...(13:30-14:59 PDT) - [What is the Right Balance of Rules for Defenders & Adversaries? Determining which dual-use model restrictions make sense and which only disarm defenders](#) - Emanuel Gawrieh,Jason Clinton,Bruce Schneier,Heather Adkins

DEF CON Talks - cont...(13:30-14:30 PDT) - [Breaking into Amazon lockers by any means necessary](#) - Martin Vigo

DEF CON Talks - (14:30-15:30 PDT) - [WASM Was Not the Boundary: Sandcastles, Not Sandboxes](#) - Saar Pearl,Vladimir "G1ND1L4" Tokarev

DEF CON Talks - [8 Out of 10 Banks in Belgium HATE This One Weird eID RCE](#) - James "Acorn221" Arnott

DEF CON Talks - cont...(13:30-14:30 PDT) - [Plug And Pwn: Weaponizing Windows PnP Auto-Install](#) - Alejandro "Oxedh" Hernando,Borja "borjnz" Martinez

DEF CON Talks - (14:30-14:59 PDT) - [Lowering the Orbit: Exploiting Satellite Protocols and communications via Software-Defined-Radio and GS](#) - Romel "r0r0x" Marin

DEF CON Talks - [Lessons from a decade of building whistleblower tech](#) - Trevor Timm,redshiftzero

DEF CON Training - cont...(08:30-17:30 PDT) - [Beat the Breach: Defend, Respond, Survive](#) - McKay Hardy,Wes Wagstaff

DEF CON Training - cont...(08:30-17:30 PDT) - [Cyber & AI Policy Basics: What Every Organization Needs in Place](#) - Pamela 'Pam' Feld,Greg Goldberg

DEF CON Training - cont...(08:30-17:30 PDT) - [Digital Supply Chain Security: Software, Cryptography, AI, and Vendor Risk](#) - Anant Shrivastava,Sunil Yadav

DEF CON Workshops - [Sold Out - Investigating and Responding to M365 account compromise on a shoestring: Living of the Land Incident Response](#) - Vince "bitpusher" Weppner

DEF CON Workshops - [Sold Out - OT Systems: how to secure them in practice!](#) - Alexandrine Torrents,Arnaud SOULLIE

DEF CON Workshops - [Sold Out - AWS Principal Threat Hunting: Behavioral Baselining for Malicious Activity](#) - Rodrigo "Sp00KeR" Montoro

DEF CON Workshops - [Sold Out - Reaching Mythos: Hands-On Vulnerability Discovery with Local AI Models](#) - John "clearbluejar" McIntosh

DEF CON Workshops - [Sold Out - Solder, Detect, Listen: Build Your Own EMF Explorer](#) - Darcy "@Drc3p0" Neal

DEF CON Workshops - [Sold Out - All About Stoopie InfoStealers: Malware Analysis for Understanding, Custom Coding for True Understanding!](#) - Ryan "@rj_chap" Chapman,Aaron "Ironical" Rosenmund

DEF CON Workshops - [Sold Out - Introduction to Malware Analysis](#) - Sam Bowne,Elizabeth Biddlecome,Kaitlyn Handelman,Irvin Lemus

DEF CON Workshops - [Sold Out - Embedded Computing Tools for Wireless Hardware Hacking](#) - Joseph Long

Demo Labs - [SecretSifter: Production Apps Are Leaking Credentials. The Blindspot DAST Never Checked.](#) - Hemanth Gorijala

Demo Labs - [MalSkill Lab: Hands-On Natural Language Malware in AI Agent Orchestration Systems](#) - Nur "BurritoTheNurrito" Gucu

Demo Labs - [Clew: Untangling Evasive Malware with Per-Sample Fuzzing Seeds](#) - Kyler McElroy,Anita Ding,Daniel Koranek

Demo Labs - [AzProwl: Prowling the Azure Attack Surface](#) - Jared "GonePhishing402" Graff,Jeff Daniels

Demo Labs - [L.A.Y.E.R.S - Layered Analysis Engine for Browser Extension Risk and Security](#) - Abhinav Khanna,Krishna Chaganti

Demo Labs - [Trajan: Cross-Platform CI/CD Security Scanner](#) - Rahul Saranjame,Ranganatha Rao Sridhar,Tanishq Rupaal

Embedded Systems Village - cont...(10:00-17:59 PDT) - [Exploit Bluetooth Low Energy with BLESPlloit and optional ESP32](#) - Slawomir Jasek

Embedded Systems Village - cont...(10:00-17:59 PDT) - [Embedded - 101 Labs](#) -

Embedded Systems Village - cont...(10:00-17:59 PDT) - [Embedded Systems Village CTF](#) -

Game Hacking Village - cont...(10:00-15:59 PDT) - [Chill Zone: Casual Games & TASBot Smash Demo](#) -

Game Hacking Village - cont...(12:00-16:59 PDT) - [Riot Games Vanguard: Pwn to own](#) -

Game Hacking Village - [iOS Game Hacking : From Zero to G0D Mode](#) - M41w4r3

Game Hacking Village - (14:45-15:45 PDT) - [Your Lives are in Another Struct: Breaking Memory Hacks with Field Relocation](#) - Ryan Zmuda

Hackers.town - [Too Much "Slop" and Not Enough Soul: Why the AI Music Bubble is Leaking & Robots Shouldn't Replace Our Djs](#) - RabidMoosery

Ham Radio Village - (14:30-15:10 PDT) - [Who Owns Your Shack? Open Source, Amateur Radio, and the Software We Can't Afford to Lose](#) - Jeremy Banker - K0JLB

ICS Village - (14:30-14:59 PDT) - [ICSForge: \(Open-Source\) OT/ICS Security Coverage Validation Platform](#) - Can Kurnaz

IoT Village - cont...(10:00-17:59 PDT) - [Expose Hidden Surveillance in Everyday Tech](#) -

IoT Village - cont...(10:00-17:59 PDT) - [Smart Home in the Matter: Blink, Race, Attack CTF](#) -

IoT Village - cont...(10:00-17:59 PDT) - [Discover GE Appliances!](#) -

IoT Village - cont...(10:00-17:59 PDT) - [Just Hacking Training](#) -

IoT Village - cont...(10:00-17:59 PDT) - [All About UART](#) -

IoT Village - cont...(10:00-17:59 PDT) - [Hands-On Hardware Hacking – From JTAG to Root, Memory Patching Boot Process for Root Access](#) -

IoT Village - cont...(10:00-17:59 PDT) - [Raiders of the Lost Firmware: A Hands-On Workshop in IoT Firmware Archaeology](#) -

IoT Village - cont...(10:00-17:59 PDT) - [Cat-astrophic Hacking: Breaking Into Smart Litter Boxes](#) -

IoT Village - cont...(13:45-15:15 PDT) - [Mesh Nets for Hackers: How \(& When\) to use Meshtastic, Meshcore, & Reticulum!](#) - Kody Kinzie

La Villa Community - [Point of Failure: Autopsia de una Terminal de Pago](#) - Erik Alcantara

La Villa Community - [PentestGPT: The Art of Hacking with Words](#) - Matias Armándola

Lockpick Village - (14:30-14:59 PDT) - [Intro to Lockpicking](#) -

Lonely Hackers Club - cont...(10:00-17:59 PDT) - [Lonely Hackers Club CTF](#) -

Lonely Hackers Club - cont...(10:00-17:59 PDT) - [Lonely Hackers Club - Lockpicking Table](#) -

Lonely Hackers Club - cont...(10:00-17:59 PDT) - [Lonely Hackers Club - Sticker Swap Table](#) -

Lonely Hackers Club - cont...(10:30-16:30 PDT) - [Resume Review with the Lonely Hackers Club](#) -

Maker's Village - cont...(10:00-17:59 PDT) - [Makers' Village - Hacker Arts and Crafts](#) -

Maker's Village - [Build-A-Badge Workshop](#) - hunny,Teazee,Buddha,MLP,M-Nelly,Alchemmer

Malware Village - [Smart Contracts, Smarter Malware: Automating Recon on Blockchain-Based C2](#) - Sai Sathvik Ruppa,Chris Navarrete

Malware Village - (14:55-15:35 PDT) - [The State of Decompiler Malware](#) - Christopher Hernandez

Malware Village - cont...(12:10-14:10 PDT) - [Introduction to Reverse Engineering With Ghidra](#) - Wesley McGrew

Malware Village - [The Achaean project-Trojan development for noobs](#) - Leigh Gilbert

Maritime Hacking Village - cont...(13:45-14:15 PDT) - [Drag, Drop, Deploy, Compromise: Why Trusted HMI Engineering Toolchains Remain an ICS Supply-Chain Blind Spot](#) - Jiwoon Yoo,TaeWoo Kim,Eunji choi

Maritime Hacking Village - (14:15-14:45 PDT) - [Scuttling Dashboards](#) - Karan Sajnani

Middle Easterns & Africans in Cyber Security (MEACS) - [The Agentic Free Pass: Does an Abliterated Backbone Make Agents Easier to Attack?](#) - Karol Piekarski,Nishith Sinha

Mobile Hacking Community - cont...(10:00-17:59 PDT) - [Mobile Hacking - Informal CTF](#) -

Mobile Hacking Community - cont...(10:00-17:59 PDT) - [Mobile Hacking Community - Open](#) -

Mobile Hacking Community - cont...(13:00-14:30 PDT) - [Hacking Android Apps in a Structured Way](#) - Sven Schleier

Nix Vegas Community - [Relocatable Nix Binaries](#) - Farid Zakaria

Noob Community - cont...(10:00-17:59 PDT) - [Skillbit Labs](#) -

Noob Community - cont...(10:00-17:59 PDT) - [TCM Security Labs](#) -

Noob Community - cont...(10:00-17:59 PDT) - [SANS Institute NetWars Labs](#) -

Noob Community - cont...(10:00-17:59 PDT) - [Mentoring and Career Advice](#) -

Noob Community - cont...(10:00-17:59 PDT) - [No Stupid Questions](#) -

Noob Community - cont...(10:00-17:59 PDT) - [Arcanum Security Labs](#) -

Noob Community - cont...(10:00-17:59 PDT) - [Hack The Box DC Junior Ranger Program Challenge](#) -

Noob Community - cont...(10:00-17:59 PDT) - [Kryptsec Labs](#) -

Noob Community - [Beyond Heatmaps: Hands-On Cyber Risk Quantification with FAIR](#) - Tony Martin-Vegue

Noob Community - (14:15-14:45 PDT) - [Day in the Life - Green Beret to AI Penetration Tester](#) - Clayton Boozell

OSINT For Good Community - cont...(13:30-14:30 PDT) - [Classical OSINT using AI \(Actual Intelligence\)](#) - Bianca C. Ionescu/reconcerto

OSINT For Good Community - cont...(10:00-17:59 PDT) - [OSINT4Good Community - DC NextGen Content](#) -

OSINT For Good Community - cont...(10:00-17:59 PDT) - [FINDX OSINT Educational Series](#) -

OSINT For Good Community - (14:30-14:59 PDT) - [Q&A with the Classical OSINT Using AI speaker](#) - Bianca C. Ionescu/reconcerto

OWASP Foundation - (14:30-15:15 PDT) - [Defend zee clankers: OWASP AI Security Verification Standard \(AISVS\)](#) - Jim Manico

OWASP Foundation - cont...(10:00-17:59 PDT) - [BadVR: Signals Everywhere a collaboration with XR Village](#) - Jad Meouchy,Suzanne Borders

OWASP Foundation - [Life Finds a Way: Secure Coding with OWASP ASVS](#) - Eden Yardeni

Packet Hacking Village - (14:30-15:30 PDT) - [Wiring the Harness: Orchestrating Frontier Models for Vulnerability Hunting at Scale](#) - Tony Martin,Arie Haenel
 Payment Village - [How to Epically Fail Your PCI Assessment](#) - Kevin Buck
 Policy @ DEF CON - [The Liability Stack: When Code Becomes Conduct](#) - Carole House
 Policy @ DEF CON - [Strengthening the CVE Ecosystem \(Seating is limited to 50 Participants\)](#) - John Banghart,Elizabeth Eigner,Lisa Olsen,Lindsey Cerkovnik
 Queercon Community - [Women Loving Women Meetup](#) -
 Radio Frequency Village - cont...(10:00-17:59 PDT) - [Radio Frequency Village Events](#) -
 Radio Frequency Village - cont...(13:30-14:25 PDT) - [Fox Hunting - Finding Rogue Access Points in the CTF and in the Wild](#) - Eric Escobar
 Radio Frequency Village - (14:30-14:55 PDT) - [Security Vulnerabilities in SATCOM Devices](#) - Aumkareshwar DS
 Recon Village - cont...(10:00-23:59 PDT) - [TrackTheFugitive Contest](#) -
 Recon Village - cont...(10:00-23:59 PDT) - [Live Recon Contest](#) -
 Recon Village - cont...(11:00-16:59 PDT) - [GE\(O\)SINT Contest](#) -
 Recon Village - cont...(12:40-15:10 PDT) - [Threat Actors: Gotta Catch 'Em All](#) - Marcelle Lee,Will Thomas
 Red Team Village - cont...(10:00-17:59 PDT) - [From Kiosk to Domain Compromise: Learning to Walk Up and Take it All](#) - Ezra Woods,Mike Manrod,Spencer Alessi
 Red Team Village - cont...(10:00-17:59 PDT) - [BloodHound Quest](#) - Hugo van den Toorn
 Red Team Village - [Cloud-Native C2: Weaponizing Trusted Infrastructure for Initial Access](#) - Dhiraj Mishra
 Red Team Village - [Quality over Quantity: How to Publish CVEs that Actually Matter](#) - Natan Morette
 Red Team Village - [Automated Mythic Deployment with Gaia](#) - Shad Brown
 Red Team Village - [Social Engineering With Reel](#) - James Williams
 Red Team Village - [Microsoft and Amazon are my Favorite C2 Providers](#) - Robert Pimentel
 Red Team Village - [Extension Hollowing: Abusing Chrome's Extension Trust Model](#) - Gordon Long
 Scambait Village - cont...(10:00-17:59 PDT) - [Open Q&A](#) -
 Scambait Village - cont...(10:00-17:59 PDT) - [KSCM Scambait Radio](#) -
 Scambait Village - [Live Call Listening](#) -
 Social Engineering Community Village - cont...(08:30-17:59 PDT) - [Social Engineering Community Village - Open Hours](#) -
 Social Engineering Community Village - cont...(13:30-14:30 PDT) - [Zero Day Hire: Can You Spot the Spy?](#) - Michael Reimsbach,Rishi "rxerium" C
 Social Gatherings/Events - cont...(08:00-18:59 PDT) - [Human Registration Open](#) -
 Social Gatherings/Events - cont...(10:00-16:59 PDT) - [Malysis: A Bare-Metal RAM Enclave for Malware Analysis. No Hypervisor. No Trace.](#) - Yannick LaRue,Samuel B. G.
 Social Gatherings/Events - cont...(10:00-16:59 PDT) - [Malysis: A Bare-Metal RAM Enclave for Malware Analysis. No Hypervisor. No Trace.](#) - Yannick LaRue,Samuel B. G.
 Social Gatherings/Events - [Book Signing - Garrett Gee](#) - Garrett Gee
 Social Gatherings/Events - [Book Signing - Laura Scherling](#) - Laura Scherling
 Social Gatherings/Events - cont...(08:00-17:59 PDT) - [Merch \(formerly swag\) Area Open -- README](#) -
 Social Gatherings/Events - cont...(10:00-18:59 PDT) - [Music - SomaFM](#) -
 Social Gatherings/Events - [Hacker Book Club Discussion](#) -
 Social Gatherings/Events - cont...(13:00-15:59 PDT) - [Free Ham Radio License Exams](#) -
 Telecom Village - (14:15-14:59 PDT) - [Protecting Humans at Machine Speed - Engineering AI to Stop Spam, Scams & Digital Fraud at Telecom Scale](#) - Arvind Singh
 The Diana Initiative - [The Diana Initiative - Open time](#) -
 Voting Village - cont...(10:00-17:59 PDT) - [Voting Village Lab](#) -
 Voting Village - [Evidence-Based Elections and Risk-Limiting Audits](#) - Philip Stark

[Adversary Village](#) - cont...(14:45-15:15 PDT) - [SEND: Teaching Machines to Lie to Defenders](#) - Yi Ting Shen, Ariz Soriano

[Adversary Village](#) - (15:15-15:45 PDT) - [Hey Adversary, I've Got a Human EDR Bypass for You...](#) - Daniel Isler

[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [ARINC 664 CTF Challenge](#) -

[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Aerospace Ecosystem Resilience Innovation Environment \(AERIE\) Cyber Range](#) -

[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Aviation ISAC Cybersecurity Challenge](#) -

[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [DCNextGen - Space Grand Challenge - SatHack: The MOUSE-1 Mission](#) -

[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Bricks in the Air](#) -

[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [DCNextGen - RIC-1: ELT Localization Exercise - N3VR-G0N Down](#) -

[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [DCNextGen - Bricks in the Air](#) -

[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Drone Hacking Choose your Own Adventure](#) -

[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Flight Simulator/EFB](#) -

[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Drone Hacking Workshop](#) -

[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [MOUSE Runner & Flappy Drone](#) -

[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Mission: Compromised - Hacking a Satellite from the Ground Up](#) -

[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Satellites Under Attack: Hands-On Satellite Security Threat Scenarios](#) -

[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [SpaceCOP - Catch Me If You Can](#) -

[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [SR-71 Blackbird Badge Challenge](#) -

[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Nebula Showdown: Space Systems Security CTF Adventure](#) -

[Aerospace Village](#) - [Drones, Detectors, and the Kill Chain](#) - Greg Albrecht

[Aerospace Village](#) - (15:30-15:59 PDT) - [Cleared for Takeoff: Debunking "Uncertifiable" Cybersecurity](#) - Katie Fejer

[AI Village](#) - cont...(10:00-17:59 PDT) - [Poster Presentations](#) -

[AI Village](#) - cont...(10:00-17:59 PDT) - [Cyber Mirage: Realtime Deepfake Demos](#) - Brandon Kovacs

[AI Village](#) - cont...(10:00-17:59 PDT) - [AI Village: Village Open](#) -

[AI Village](#) - [Pwning the Internet of Agents: Zero-Click Backdoors in OpenClaw and a Global Agent Botnet on MoltBook](#) - João Maria Campos Donato, Stav Cohen

[AppSec Village](#) - (15:15-16:15 PDT) - [IDEViewer - Securing Developer Workstations from IDE Supply Chain Threats](#) - securient

[AppSec Village](#) - cont...(14:30-16:59 PDT) - [Container Escapes 101](#) - some-natalie

[AppSec Village](#) - cont...(14:50-15:20 PDT) - [GeoHacking: from memory corruption RCE to cross tenant access](#) - Michal Kamensky

[AppSec Village](#) - (15:30-15:59 PDT) - [Zero Trust Kubernetes Security: Preventing Real World Container Attacks](#) - Janakiram Meka

[AppSec Village](#) - [Cards Against Vulnerabilities](#) - Patrick Smyth

[AppSec Village](#) - [AI Pentesting Trivia Showdown](#) - Andy Dennis, Bill Reyor

[AppSec Village](#) - [SBOM Find the Flaws](#) - Dmitry Raidman

[AppSec Village](#) - [NPM Imposters - The malware detection card game](#) - Mackenzie

[Biohacking Village](#) - cont...(10:00-17:59 PDT) - [Biohacking Device Lab](#) -

[Biohacking Village](#) - cont...(10:00-17:59 PDT) - [Embedded & Shredded: Advanced Embedded System Hacking](#) -

[Biohacking Village](#) - (15:45-16:30 PDT) - [Snap, Crackle, Popped: How to manage a massive cyber attack](#) - David Nathans

[Blacks In Cyber Village](#) - [The Cost of Unverified Intelligence: AI and Accountability in Defense Operations](#) - Kayrene Woods

[Blacks In Cyber Village](#) - (15:30-15:55 PDT) - [Configuring Your Favorite Platforms to Prioritize DNS](#) - Malachi Walker, Anthony Johnson

[Blue Team Village](#) - cont...(14:30-15:30 PDT) - [Building Project Obsidian: Designing the Blue Team CTF for DEF CON](#) - Carlo Anez Mazurco, Chris "dafinga" Maenner, Omenscan ~, Paul Goffar

[Blue Team Village](#) - (15:45-16:45 PDT) - [The Modern Detection Engineer](#) - Alex Hurtado, Chase Phelps, Chris Kulakowski, Christina Parry, Zack Allen

[Bug Bounty Village](#) - [Cache Key Injection: Smuggling Poison Through the Door](#) - Alex Brumen

[Bug Bounty Village](#) - (15:30-15:59 PDT) - [Hunting for Cryptographic Ghosts: A Bug Hunter's Guide to Signature Malleability and Replay Attacks in EVM Bridges & Multi-Sigs](#) - Samet Berk Simsek, Ahmet Furkan Aydogan

[Bug Bounty Village](#) - [a \[REDACTED\] history of this hobby](#) - Chris "flyingtoasters" Holt, Michael Skelton

[Call Center Village](#) - cont...(10:00-17:59 PDT) - [Call Center Village](#) - Open -
[Call Center Village](#) - [An Intrusion in the Living Room is now an international incident: SuperBOX Part 3](#) - D3adA55
[Car Hacking Village](#) - cont...(10:00-16:59 PDT) - [Bomb Bot Challenge](#) -
[Car Hacking Village](#) - cont...(10:00-17:59 PDT) - [Car Hacking Village Open](#) -
[Cloud Village](#) - cont...(13:30-15:30 PDT) - [Cloudy with a Chance of Breaches: Hands-On AWS Threat Defense](#) - Kyle Hubbard
[Cloud Village](#) - cont...(14:30-15:10 PDT) - [Citizen Developers Can't Defend What They Built: Scaling Security Past the Security Team](#) -
[Cloud Village](#) - [Go with the Flow: Riding GCP Dataflow Shadow Dependency to Cross-Tenant Compromise](#) - Gil Weizman,Tamir Yehuda
[Cloud Village](#) - (15:30-16:10 PDT) - [The Polymorphic Agent: From Cross Agent Escalation to Just in Time Defense on Azure](#) - Muskan Tomar
[CodeBloom](#) - [Game Time: Input, Output, and Variables](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [5N4CK3Y](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [DC's Next Top Threat Model](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Untechnical](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [DEF CON Scavenger Hunt](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Darknet-NG](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Crack Me If You Can 2026](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [TeleChallenge](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [HackFortress](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [?Cube](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [\\$unL1ght Sh4d0w5](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Octopus Game](#) - Booth Open -
[Contests](#) - cont...(10:00-17:59 PDT) - [Beer Chilling Contraption Contest](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Cryptid Hunt](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [HSPACE: AI Battlegrounds](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [spyVspy 3: Rat Race](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Hacker Games](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [PhreakMe](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Game Hacking Village CTF](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Kubernetes CTF](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Hac-Man](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Crack the Core](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Cyber Deck Competition](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Pinball High Score Contest](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Code Cadaver: Break Every System. Save Your Friend.](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [PWN UR H0M3 - DDoS CTF](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Real7y Overrun](#) - Contest running -
[Contests](#) - cont...(10:00-17:59 PDT) - [Tin Foil Hat Contest](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [CMD+CTRL Cyber Range: DarkMoney](#) -
[Contests](#) - cont...(13:00-17:59 PDT) - [Locktopus](#) - Open Qualifying -
[Contests](#) - cont...(11:00-17:59 PDT) - [Radio Frequency Capture the Flag](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [DEF CON CTF: Benevolent Bureau of Birds](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [AI Village](#) - Hal CTF -
[Contests](#) - cont...(10:00-17:59 PDT) - [AI Village Plays Pokemon: DEFCON Edition](#) - Nick Ashworth
[Contests](#) - cont...(10:00-16:59 PDT) - [Car Hacking Village CTF](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [OWASP CTF](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Escalation Desk CTF](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [DEF CON Groups Sticker Contest](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [DEF CON Groups Backdoors & Breaches](#) - Tim Doerges,Seth Benning
[Contests](#) - cont...(10:00-23:59 PDT) - [Apex Park \(Cloud Village CTF\)](#) -
[Contests](#) - cont...(13:00-15:59 PDT) - [SEC Vishing Competition \(SECVC\)](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Hacking GRC Contest](#) -
[Crypto & Privacy Village](#) - (15:45-16:30 PDT) - [Step Zero: Identifying the Quantum Attack Surface in Critical Infrastructure](#) -

Dr. Katrina Rosseini, Dr. Allan Friedman

[Data Duplication Village](#) - cont...(10:00-17:59 PDT) - [DDV open and accepting drives for duplication](#) -

[DCNextGen - Level Up](#) - [Could your Gaming Talents be Perfect for a Career in Cyber Security?](#) - The Hacking Games

[DEF CON Groups](#) - cont...(10:00-17:59 PDT) - [DEF CON Groups \(DCG\)](#) -

[DEF CON Talks](#) - [The Stream Is Dead, Long Live the Stream: How HTTP/2 Lets Dead Streams Keep Servers Working](#) - Gal Bar Nahum

[DEF CON Talks](#) - cont...(14:30-15:30 PDT) - [WASM Was Not the Boundary: Sandcastles, Not Sandboxes](#) - Saar

Pearl, Vladimir "G1ND1L4" Tokarev

[DEF CON Talks](#) - (15:30-16:30 PDT) - [Your Bank Thinks I'm You: A Complete Kill Chain Against Mobile Banking Security](#)

- Xavier "@xaferima" Riofrio Machado, Alex Tipan

[DEF CON Talks](#) - [Hacking the Hackers who Hack Hackers: Supply-Chain Backdoors in Underground VPN Infrastructure](#) - Assaf Morag

[DEF CON Talks](#) - [Pwning Rekordbox: Unauthenticated filesystem access in the world's most popular DJ software](#) -

Christopher "TRIODE" Le

[DEF CON Talks](#) - (15:30-16:30 PDT) - [Riding for Free - Breaking Public Transport RFID at Scale](#) - Aidan "luu176" Nakache

[DEF CON Talks](#) - [Data Tomb Raider: Raiding Modern AI Vaults with Legacy Flaws for Treasure Stealing](#) - Dolev

Taler, Mark Vaitsman

[DEF CON Training](#) - cont...(08:30-17:30 PDT) - [Beat the Breach: Defend, Respond, Survive](#) - McKay Hardy, Wes Wagstaff

[DEF CON Training](#) - cont...(08:30-17:30 PDT) - [Cyber & AI Policy Basics: What Every Organization Needs in Place](#) -

Pamela 'Pam' Feld, Greg Goldberg

[DEF CON Training](#) - cont...(08:30-17:30 PDT) - [Digital Supply Chain Security: Software, Cryptography, AI, and Vendor Risk](#) - Anant Shrivastava, Sunil Yadav

[DEF CON Workshops](#) - cont...(14:00-17:59 PDT) - [Sold Out - Investigating and Responding to M365 account compromise on a shoestring: Living of the Land Incident Response](#) - Vince "bitpusher" Weppner

[DEF CON Workshops](#) - cont...(14:00-17:59 PDT) - [Sold Out - OT Systems: how to secure them in practice!](#) - Alexandrine Torrents, Arnaud SOULLIE

[DEF CON Workshops](#) - cont...(14:00-17:59 PDT) - [Sold Out - AWS Principal Threat Hunting: Behavioral Baselining for Malicious Activity](#) - Rodrigo "Sp0oKeR" Montoro

[DEF CON Workshops](#) - cont...(14:00-17:59 PDT) - [Sold Out - Reaching Mythos: Hands-On Vulnerability Discovery with Local AI Models](#) - John "clearbluejar" McIntosh

[DEF CON Workshops](#) - cont...(14:00-17:59 PDT) - [Sold Out - Solder, Detect, Listen: Build Your Own EMF Explorer](#) - Darcy "@Drc3p0" Neal

[DEF CON Workshops](#) - cont...(14:00-17:59 PDT) - [Sold Out - All About Stoopie InfoStealers: Malware Analysis for Understanding, Custom Coding for True Understanding!](#) - Ryan "@rj_chap" Chapman, Aaron "Ironical" Rosenmund

[DEF CON Workshops](#) - cont...(14:00-17:59 PDT) - [Sold Out - Introduction to Malware Analysis](#) - Sam Bowne, Elizabeth Biddlecome, Kaitlyn Handelman, Irvin Lemus

[DEF CON Workshops](#) - cont...(14:00-17:59 PDT) - [Sold Out - Embedded Computing Tools for Wireless Hardware Hacking](#) - Joseph Long

[Demo Labs](#) - [GhostCatcher \(endpoint detection agent\)](#) - Sercan Okur

[Demo Labs](#) - [Intercept.js: Runtime-Aware Detection for JavaScript Environments](#) - Rishi Kant

[Demo Labs](#) - [BigIron.ai: AI-Assisted Exploration and Security Analysis of Mainframe Systems](#) - Adam "w00t0ck" Toscher

[Demo Labs](#) - [AzProwl: Prowling the Azure Attack Surface](#) - Jared "GonePhishing402" Graff, Jeff Daniels

[Demo Labs](#) - [TokenMesh: Exposing Azure's Hidden Identity Attack Surface](#) - Saksham Agrawal

[Demo Labs](#) - [pymSI: Interactive MSI Installer Analysis in Python and the Browser](#) - Ryan "Nightlark" Mast

[Embedded Systems Village](#) - cont...(10:00-17:59 PDT) - [Exploit Bluetooth Low Energy with BLESPloit and optional ESP32](#) - Slawomir Jasek

[Embedded Systems Village](#) - cont...(10:00-17:59 PDT) - [Embedded - 101 Labs](#) -

[Embedded Systems Village](#) - cont...(10:00-17:59 PDT) - [Embedded Systems Village CTF](#) -

[Game Hacking Village](#) - cont...(10:00-15:59 PDT) - [Chill Zone: Casual Games & TASBot Smash Demo](#) -

[Game Hacking Village](#) - cont...(12:00-16:59 PDT) - [Riot Games Vanguard: Pwn to own](#) -

[Game Hacking Village](#) - cont...(14:45-15:45 PDT) - [Your Lives are in Another Struct: Breaking Memory Hacks with Field Relocation](#) - Ryan Zmuda

[Hackers.town](#) - [The Political economy of AI](#) - Janet Vertesi

[Ham Radio Village](#) - cont...(14:30-15:10 PDT) - [Who Owns Your Shack? Open Source, Amateur Radio, and the Software We Can't Afford to Lose](#) - Jeremy Banker - K0JLB

[Ham Radio Village](#) - (15:30-16:18 PDT) - [Advanced Topics in LoRa Meshes](#) - Eric Escobar
[ICS Village](#) - [OT Segmentation Under Operational Constraints](#) - Tony Turner
[IoT Village](#) - cont...(10:00-17:59 PDT) - [Discover GE Appliances!](#) -
[IoT Village](#) - cont...(10:00-17:59 PDT) - [Smart Home in the Matter: Blink, Race, Attack CTF](#) -
[IoT Village](#) - cont...(10:00-17:59 PDT) - [Expose Hidden Surveillance in Everyday Tech](#) -
[IoT Village](#) - cont...(10:00-17:59 PDT) - [Cat-apstrophic Hacking: Breaking Into Smart Litter Boxes](#) -
[IoT Village](#) - cont...(10:00-17:59 PDT) - [Hands-On Hardware Hacking – From JTAG to Root, Memory Patching Boot Process for Root Access](#) -
[IoT Village](#) - cont...(10:00-17:59 PDT) - [All About UART](#) -
[IoT Village](#) - cont...(10:00-17:59 PDT) - [Just Hacking Training](#) -
[IoT Village](#) - cont...(10:00-17:59 PDT) - [Raiders of the Lost Firmware: A Hands-On Workshop in IoT Firmware Archaeology](#) -
[IoT Village](#) - cont...(13:45-15:15 PDT) - [Mesh Nets for Hackers: How \(& When\) to use Meshtastic, Meshcore, & Reticulum!](#) - Kody Kinzie
[IoT Village](#) - (15:45-17:15 PDT) - [Wi-Fi Self Defense & Hacker Hunting & For Beginners](#) - Kody Kinzie
[La Villa Community](#) - [El regreso de Sedinho: situación actual y nuevas tácticas de los troyanos bancarios brasileños](#) - Josep Albors
[La Villa Community](#) - (15:30-15:59 PDT) - [State Desync as a Weapon: Breaking Transactional Integrity in Payment Systems \(ESP\)](#) - Santiago Sepúlveda Veliz
[La Villa Community](#) - cont...(14:00-15:59 PDT) - [PentestGPT: The Art of Hacking with Words](#) - Matias Armándola
[Lonely Hackers Club](#) - cont...(10:00-17:59 PDT) - [Lonely Hackers Club CTF](#) -
[Lonely Hackers Club](#) - cont...(10:00-17:59 PDT) - [Lonely Hackers Club - Lockpicking Table](#) -
[Lonely Hackers Club](#) - cont...(10:00-17:59 PDT) - [Lonely Hackers Club - Sticker Swap Table](#) -
[Lonely Hackers Club](#) - cont...(10:30-16:30 PDT) - [Resume Review with the Lonely Hackers Club](#) -
[Maker's Village](#) - cont...(10:00-17:59 PDT) - [Makers' Village - Hacker Arts and Crafts](#) -
[Maker's Village](#) - cont...(14:00-15:30 PDT) - [Build-A-Badge Workshop](#) - hunny,Teazee,Buddha,MLP,M-Nelly,Alchemmer
[Maker's Village](#) - [Cyberdeck Build](#) - Sk!tz0
[Malware Village](#) - cont...(14:55-15:35 PDT) - [The State of Decompiler Malware](#) - Christopher Hernandez
[Malware Village](#) - (15:45-16:25 PDT) - [Vibe Check: Exploiting Developer Trust from Prompt Injections to Weaponized Repos](#) - Michael Chan
[Malware Village](#) - cont...(14:10-17:25 PDT) - [The Achaean project-Trojan development for noobs](#) - Leigh Gilbert
[Middle Easterns & Africans in Cyber Security \(MEACS\)](#) - [The New Horizons in Quantum and Space](#) - Anshu Gupta
[Misc](#) - (15:30-16:30 PDT) - [tAIrot Readings](#) -
[Mobile Hacking Community](#) - cont...(10:00-17:59 PDT) - [Mobile Hacking - Informal CTF](#) -
[Mobile Hacking Community](#) - cont...(10:00-17:59 PDT) - [Mobile Hacking Community - Open](#) -
[Mobile Hacking Community](#) - [Mobile Security through Obscurity, from insecure client-side encryption to unauthenticated SQL](#) - Juan Urbano Stordeur,Juan Martinez Blanco
[Nix Vegas Community](#) - [Everything is Nix when you squint hard enough](#) - Jared
[Noob Community](#) - cont...(10:00-17:59 PDT) - [Skillbit Labs](#) -
[Noob Community](#) - cont...(10:00-17:59 PDT) - [SANS Institute NetWars Labs](#) -
[Noob Community](#) - cont...(10:00-17:59 PDT) - [TCM Security Labs](#) -
[Noob Community](#) - cont...(10:00-17:59 PDT) - [Hack The Box DC Junior Ranger Program Challenge](#) -
[Noob Community](#) - cont...(10:00-17:59 PDT) - [Arcanum Security Labs](#) -
[Noob Community](#) - cont...(10:00-17:59 PDT) - [Kryptsec Labs](#) -
[Noob Community](#) - cont...(10:00-17:59 PDT) - [No Stupid Questions](#) -
[Noob Community](#) - cont...(10:00-17:59 PDT) - [Mentoring and Career Advice](#) -
[Noob Community](#) - cont...(14:00-15:20 PDT) - [Beyond Heatmaps: Hands-On Cyber Risk Quantification with FAIR](#) - Tony Martin-Vegue
[Noob Community](#) - [The impact of CTF Write-Ups](#) - Mathias Detmers
[Noob Community](#) - (15:30-16:59 PDT) - [Introduction to Web Exploitation](#) - Roman Bohuk
[Noob Community](#) - (15:30-15:45 PDT) - [Lessons Learned From A Decade of Resumes](#) - Britt Kemp
[OSINT For Good Community](#) - cont...(10:00-17:59 PDT) - [FINDX OSINT Educational Series](#) -
[OSINT For Good Community](#) - cont...(10:00-17:59 PDT) - [OSINT4Good Community - DC NextGen Content](#) -
[OSINT For Good Community](#) - (15:30-16:30 PDT) - [Trace Labs L100: Search Party Basics](#) - Sarah "scba" Miller
[OWASP Foundation](#) - cont...(14:30-15:15 PDT) - [Defend zee clankers: OWASP AI Security Verification Standard \(AISVS\)](#) -

Jim Manico

[OWASP Foundation](#) - (15:15-15:59 PDT) - [Forged in fire: Malware Factory](#) - Jon McCoy, Andra Lezza
[OWASP Foundation](#) - cont...(10:00-17:59 PDT) - [BadVR: Signals Everywhere a collaboration with XR Village](#) - Jad Meouchy, Suzanne Borders
[OWASP Foundation](#) - cont...(14:00-15:59 PDT) - [Life Finds a Way: Secure Coding with OWASP ASVS](#) - Eden Yardeni
[Packet Hacking Village](#) - cont...(14:30-15:30 PDT) - [Wiring the Harness: Orchestrating Frontier Models for Vulnerability Hunting at Scale](#) - Tony Martin, Arie Haenel
[Payment Village](#) - [Deepfake Detection Through Adversarial Research](#) - Efim Boieru
[Physical Security Village](#) - (15:30-15:59 PDT) - [Forensics of Covert Entry](#) - Bill Graydon, Bobby Graydon
[Policy @ DEF CON](#) - (15:30-16:30 PDT) - [Privacy's Defender: How Hackers Protected the Internet Before and Can Do It Again](#) - Cindy Cohn
[Policy @ DEF CON](#) - cont...(14:00-15:30 PDT) - [Strengthening the CVE Ecosystem \(Seating is limited to 50 Participants\)](#) - John Banghart, Elizabeth Eigner, Lisa Olsen, Lindsey Cerkovnik
[Policy @ DEF CON](#) - (15:30-16:30 PDT) - [When AI Finds Everything: Vulnerability Policy for the Coming Discovery Surge](#) - Alec Summers, Lindsey Cerkovnik, Madison Ficorelli
[Queercon Community](#) - [Furs and Kinksters Meetup](#) -
[Radio Frequency Village](#) - cont...(10:00-17:59 PDT) - [Radio Frequency Village Events](#) -
[Radio Frequency Village](#) - [Hack the Planet \(not ours\)](#) - Abraxas3d
[Radio Frequency Village](#) - (15:30-16:25 PDT) - [AI-assisted RF Hacking with GNU Radio](#) - Erwin Karincic (Dollarhyde)
[Recon Village](#) - cont...(10:00-23:59 PDT) - [TrackTheFugitive Contest](#) -
[Recon Village](#) - cont...(10:00-23:59 PDT) - [Live Recon Contest](#) -
[Recon Village](#) - cont...(11:00-16:59 PDT) - [GE\(O\)SINT Contest](#) -
[Recon Village](#) - cont...(12:40-15:10 PDT) - [Threat Actors: Gotta Catch 'Em All](#) - Marcelle Lee, Will Thomas
[Recon Village](#) - (15:30-17:59 PDT) - [BBOT: Automating the OSINT Kill Chain with a Single Command](#) - Mark Gaddy
[Red Team Village](#) - cont...(10:00-17:59 PDT) - [From Kiosk to Domain Compromise: Learning to Walk Up and Take it All](#) - Ezra Woods, Mike Manrod, Spencer Alessi
[Red Team Village](#) - cont...(10:00-17:59 PDT) - [BloodHound Quest](#) - Hugo van den Toorn
[Red Team Village](#) - cont...(14:00-15:59 PDT) - [Cloud-Native C2: Weaponizing Trusted Infrastructure for Initial Access](#) - Dhiraj Mishra
[Red Team Village](#) - cont...(14:00-15:59 PDT) - [Quality over Quantity: How to Publish CVEs that Actually Matter](#) - Natan Morette
[Red Team Village](#) - cont...(14:00-15:59 PDT) - [Automated Mythic Deployment with Gaia](#) - Shad Brown
[Red Team Village](#) - cont...(14:00-15:59 PDT) - [Social Engineering With Reel](#) - James Williams
[Red Team Village](#) - [Trust the Pipeline, Lose the Kingdom: Hands-On Cloud Native CI/CD Red Team](#) - Shane Young
[Red Team Village](#) - [LLM-Coached Red Team Tactics to Attack Zero Trust](#) - Rudy Ristich, Vijay Anand
[Scambait Village](#) - cont...(10:00-17:59 PDT) - [Open Q&A](#) -
[Scambait Village](#) - cont...(10:00-17:59 PDT) - [KSCM Scambait Radio](#) -
[Scambait Village](#) - cont...(14:00-17:59 PDT) - [Live Call Listening](#) -
[Social Engineering Community Village](#) - cont...(08:30-17:59 PDT) - [Social Engineering Community Village - Open Hours](#) -
[Social Engineering Community Village](#) - (15:30-16:59 PDT) - [SE Improv](#) - Bryan, Kevin
[Social Gatherings/Events](#) - cont...(08:00-18:59 PDT) - [Human Registration Open](#) -
[Social Gatherings/Events](#) - [Book Signing](#) - Ted Harrington - Ted Harrington
[Social Gatherings/Events](#) - cont...(10:00-16:59 PDT) - [Malysis: A Bare-Metal RAM Enclave for Malware Analysis. No Hypervisor. No Trace.](#) - Yannick LaRue, Samuel B. G.
[Social Gatherings/Events](#) - cont...(10:00-16:59 PDT) - [Malysis: A Bare-Metal RAM Enclave for Malware Analysis. No Hypervisor. No Trace.](#) - Yannick LaRue, Samuel B. G.
[Social Gatherings/Events](#) - [Book Signing](#) - Avinash Majeti - Avinash Majeti
[Social Gatherings/Events](#) - cont...(14:00-15:59 PDT) - [Book Signing](#) - Laura Scherling - Laura Scherling
[Social Gatherings/Events](#) - cont...(08:00-17:59 PDT) - [Merch \(formerly swag\) Area Open -- README](#) -
[Social Gatherings/Events](#) - cont...(10:00-18:59 PDT) - [Music](#) - SomaFM -
[Social Gatherings/Events](#) - cont...(14:00-15:59 PDT) - [Hacker Book Club Discussion](#) -
[Social Gatherings/Events](#) - cont...(13:00-15:59 PDT) - [Free Ham Radio License Exams](#) -
[Telecom Village](#) - [SIM Card Strikes Back: Telecom Threats & SOC Detection](#) - Zibran Sayyed
[Telecom Village](#) - (15:30-15:59 PDT) - [AI vs AI: Securing Telecom in the Era of Autonomous Cyber Warfare](#) - Rohini, Pankaj Sontakke, Will Thomas, Isabel Manjarrez, Omer Farooq, T -Mobile CTF Team, James(GSMA), Arvind Singh

[The Diana Initiative - Dear Red Team, Love Blue Team: Pulling Both Screaming Parties into Purple](#) - Allie
[Voting Village](#) - cont...(10:00-17:59 PDT) - [Voting Village Lab](#) -
[Voting Village](#) - (15:30-15:59 PDT) - [There and Back Again](#) - Jason Wareham,Manbir Gulati

[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Satellites Under Attack: Hands-On Satellite Security Threat Scenarios](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [SpaceCOP - Catch Me If You Can](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Nebula Showdown: Space Systems Security CTF Adventure](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [SR-71 Blackbird Badge Challenge](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Mission: Compromised - Hacking a Satellite from the Ground Up](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Drone Hacking Choose your Own Adventure](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Drone Hacking Workshop](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [MOUSE Runner & Flappy Drone](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Flight Simulator/EFB](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [ARINC 664 CTF Challenge](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Aerospace Ecosystem Resilience Innovation Environment \(AERIE\) Cyber Range](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Bricks in the Air](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Aviation ISAC Cybersecurity Challenge](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [DCNextGen - Space Grand Challenge - SatHack: The MOUSE-1 Mission](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [DCNextGen - RIC-1: ELT Localization Exercise - N3VR-G0N Down](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [DCNextGen - Bricks in the Air](#) -
[AI Village](#) - cont...(10:00-17:59 PDT) - [AI Village: Village Open](#) -
[AI Village](#) - cont...(10:00-17:59 PDT) - [Cyber Mirage: Realtime Deepfake Demos](#) - Brandon Kovacs
[AI Village](#) - cont...(10:00-17:59 PDT) - [Poster Presentations](#) -
[AI Village](#) - [Bruce's Fireside Chat](#) - Bruce Schneier
[AI Village](#) - (16:30-16:59 PDT) - [Minimize Harm, Maximize Defense: How Anthropic Navigates the Offense-Defense Divide](#) - Curt Barnard
[AppSec Village](#) - cont...(15:15-16:15 PDT) - [IDEViewer - Securing Developer Workstations from IDE Supply Chain Threats](#) - securient
[AppSec Village](#) - (16:30-17:30 PDT) - [Rebuilding Code Security with Signal, Speed and AI](#) - Derek C.,Shasheen Bandodkar
[AppSec Village](#) - cont...(14:30-16:59 PDT) - [Container Escapes 101](#) - some-natalie
[AppSec Village](#) - [Man-in-the-Browser: Hijacking Javascript APIs for Browser Persistence and Credential Theft](#) - Aarav Juneja
[AppSec Village](#) - (16:50-17:20 PDT) - [Most threat modeling artifacts don't help coding agents fix business logic. Here's what does.](#) - Meitar Ronen
[AppSec Village](#) - cont...(15:00-16:59 PDT) - [Cards Against Vulnerabilities](#) - Patrick Smyth
[AppSec Village](#) - cont...(15:00-16:59 PDT) - [AI Pentesting Trivia Showdown](#) - Andy Dennis,Bill Reyor
[AppSec Village](#) - cont...(15:00-16:59 PDT) - [SBOM Find the Flaws](#) - Dmitry Raidman
[AppSec Village](#) - cont...(15:00-16:59 PDT) - [NPM Imposters - The malware detection card game](#) - Mackenzie
[Biohacking Village](#) - cont...(10:00-17:59 PDT) - [Biohacking Device Lab](#) -
[Biohacking Village](#) - cont...(10:00-17:59 PDT) - [Embedded & Shredded: Advanced Embedded System Hacking](#) -
[Biohacking Village](#) - cont...(15:45-16:30 PDT) - [Snap, Crackle, Popped: How to manage a massive cyber attack](#) - David Nathans
[Biohacking Village](#) - (16:30-17:15 PDT) - [Lights Out and Last Call: A Drunken Tabletop on Medical Device Resilience](#) - Courtney McCarty
[Blacks In Cyber Village](#) - [KaliGPT Vibe-Ethical Hacking Session](#) - Timothy E. Bates
[Blue Team Village](#) - cont...(15:45-16:45 PDT) - [The Modern Detection Engineer](#) - Alex Hurtado,Chase Phelps,Chris Kulakowski,Christina Parry,Zack Allen
[Bug Bounty Village](#) - [Hacking Human-in-the-Loop systems](#) - Inti "securinti" De Ceukelaire
[Call Center Village](#) - cont...(10:00-17:59 PDT) - [Call Center Village - Open](#) -
[Car Hacking Village](#) - cont...(10:00-16:59 PDT) - [Bomb Bot Challenge](#) -
[Car Hacking Village](#) - cont...(10:00-17:59 PDT) - [Car Hacking Village Open](#) -
[Cloud Village](#) - [Cirro: Extending Your Azure Graph Beyond Identities](#) - Leron Gray
[Cloud Village](#) - [From Dashboard to Exploit: Weaponizing and Winning the Cloud Queue](#) - Mackenzie Jackson
[Cloud Village](#) - cont...(15:30-16:10 PDT) - [The Polymorphic Agent: From Cross Agent Escalation to Just in Time Defense on Azure](#) - Muskan Tomar

[Cloud Village - The New Software Supply Chain Nobody is Securing: MCP](#) -
[Cloud Village - \(16:50-17:30 PDT\) - Trust Fall: How Agentic AI Inherits Your Cloud's Worst IAM Habits](#) - Aravind Sreekanth Pallavoor,Sadhana Sainarayanan
[CodeBloom - What is AI?](#) - Sam Mosley
[Contests - Um, ACKtually](#) -
[Contests - cont...\(10:00-17:59 PDT\) - 5N4CK3Y](#) -
[Contests - cont...\(10:00-17:59 PDT\) - DC's Next Top Threat Model](#) -
[Contests - cont...\(10:00-17:59 PDT\) - Untechnical](#) -
[Contests - cont...\(10:00-17:59 PDT\) - DEF CON Scavenger Hunt](#) -
[Contests - cont...\(10:00-17:59 PDT\) - Darknet-NG](#) -
[Contests - cont...\(10:00-17:59 PDT\) - Crack Me If You Can 2026](#) -
[Contests - cont...\(10:00-17:59 PDT\) - TeleChallenge](#) -
[Contests - cont...\(10:00-17:59 PDT\) - HackFortress](#) -
[Contests - cont...\(10:00-17:59 PDT\) - ?Cube](#) -
[Contests - cont...\(10:00-17:59 PDT\) - \\$unLight Sh4d0w5](#) -
[Contests - cont...\(10:00-17:59 PDT\) - Octopus Game - Booth Open](#) -
[Contests - cont...\(10:00-17:59 PDT\) - Beer Chilling Contraption Contest](#) -
[Contests - cont...\(10:00-17:59 PDT\) - Cryptid Hunt](#) -
[Contests - cont...\(10:00-17:59 PDT\) - HSPACE: AI Battlegrounds](#) -
[Contests - cont...\(10:00-17:59 PDT\) - spyVspy 3: Rat Race](#) -
[Contests - cont...\(10:00-17:59 PDT\) - Hacker Games](#) -
[Contests - cont...\(10:00-17:59 PDT\) - PhreakMe](#) -
[Contests - cont...\(10:00-17:59 PDT\) - Game Hacking Village CTF](#) -
[Contests - cont...\(10:00-17:59 PDT\) - Kubernetes CTF](#) -
[Contests - cont...\(10:00-17:59 PDT\) - Hac-Man](#) -
[Contests - cont...\(10:00-17:59 PDT\) - Crack the Core](#) -
[Contests - cont...\(10:00-17:59 PDT\) - Cyber Deck Competition](#) -
[Contests - cont...\(10:00-17:59 PDT\) - Pinball High Score Contest](#) -
[Contests - cont...\(10:00-17:59 PDT\) - Code Cadaver: Break Every System. Save Your Friend.](#) -
[Contests - cont...\(10:00-17:59 PDT\) - PWN UR H0M3 - DDoS CTF](#) -
[Contests - cont...\(10:00-17:59 PDT\) - Reali7y Overrun - Contest running](#) -
[Contests - cont...\(10:00-17:59 PDT\) - Tin Foil Hat Contest](#) -
[Contests - cont...\(10:00-17:59 PDT\) - CMD+CTRL Cyber Range: DarkMoney](#) -
[Contests - cont...\(13:00-17:59 PDT\) - Locktopus - Open Qualifying](#) -
[Contests - cont...\(11:00-17:59 PDT\) - Radio Frequency Capture the Flag](#) -
[Contests - cont...\(10:00-17:59 PDT\) - DEF CON CTF: Benevolent Bureau of Birds](#) -
[Contests - cont...\(10:00-17:59 PDT\) - AI Village - Hal CTF](#) -
[Contests - cont...\(10:00-17:59 PDT\) - AI Village Plays Pokemon: DEFCON Edition](#) - Nick Ashworth
[Contests - cont...\(10:00-16:59 PDT\) - Car Hacking Village CTF](#) -
[Contests - cont...\(10:00-17:59 PDT\) - OWASP CTF](#) -
[Contests - cont...\(10:00-17:59 PDT\) - Escalation Desk CTF](#) -
[Contests - cont...\(10:00-17:59 PDT\) - DEF CON Groups Sticker Contest](#) -
[Contests - cont...\(10:00-17:59 PDT\) - DEF CON Groups Backdoors & Breaches](#) - Tim Doerges,Seth Benning
[Contests - cont...\(10:00-23:59 PDT\) - Apex Park \(Cloud Village CTF\)](#) -
[Contests - cont...\(10:00-17:59 PDT\) - Hacking GRC Contest](#) -
[Crypto & Privacy Village - cont...\(15:45-16:30 PDT\) - Step Zero: Identifying the Quantum Attack Surface in Critical Infrastructure](#) - Dr. Katrina Rosseini,Dr. Allan Friedman
[Crypto & Privacy Village - \(16:30-17:15 PDT\) - Crypto Is Fine. The Code Is Not: Real-World Cryptographic Failures](#) - Diptendu Kar
[Data Duplication Village - cont...\(10:00-17:59 PDT\) - DDV open and accepting drives for duplication](#) -
[DCNextGen - Veilid- the Next Gen of privacy](#) - medus4
[DEF CON Groups - cont...\(10:00-17:59 PDT\) - DEF CON Groups \(DCG\)](#) -
[DEF CON Talks - The Sandbox is a Suggestion: Deconstructing AI Agent Sandboxes](#) - Elad Meged
[DEF CON Talks - cont...\(15:30-16:30 PDT\) - Your Bank Thinks I'm You: A Complete Kill Chain Against Mobile Banking Security](#) - Xavier "@xaferima" Riofrio Machado,Alex Tipan

DEF CON Talks - (16:30-17:30 PDT) - [noRecognition: Could a pattern on your clothing fool Facial Facial Recognition?](#) - Bill "hevnsnt" Swearingen

DEF CON Talks - [Hacking the EOD Bot: How I Learned to Stop Worrying and Love the Boomba](#) - Patrick "gigstorm" Kiley,Emily "@astradotpng" Astranova

DEF CON Talks - cont...(15:30-16:30 PDT) - [Riding for Free - Breaking Public Transport RFID at Scale](#) - Aidan "luu176" Nakache

DEF CON Talks - (16:30-17:30 PDT) - [CloudBashing: Exploiting free CloudShells for mining, networking, exfil, and persistence at scale](#) - Jenko "edleft" Hwong,Chris Ryan

DEF CON Talks - [Certified Re-Pwned: escalating all the way up](#) - Daniel Monzon,Eric Labrador

DEF CON Training - cont...(08:30-17:30 PDT) - [Beat the Breach: Defend, Respond, Survive](#) - McKay Hardy,Wes Wagstaff

DEF CON Training - cont...(08:30-17:30 PDT) - [Cyber & AI Policy Basics: What Every Organization Needs in Place](#) - Pamela 'Pam' Feld,Greg Goldberg

DEF CON Training - cont...(08:30-17:30 PDT) - [Digital Supply Chain Security: Software, Cryptography, AI, and Vendor Risk](#) - Anant Shrivastava,Sunil Yadav

DEF CON Workshops - cont...(14:00-17:59 PDT) - [Sold Out - Investigating and Responding to M365 account compromise on a shoestring: Living of the Land Incident Response](#) - Vince "bitpusher" Weppner

DEF CON Workshops - cont...(14:00-17:59 PDT) - [Sold Out - OT Systems: how to secure them in practice!](#) - Alexandrine Torrents,Arnaud SOULLIE

DEF CON Workshops - cont...(14:00-17:59 PDT) - [Sold Out - AWS Principal Threat Hunting: Behavioral Baselining for Malicious Activity](#) - Rodrigo "Sp0oKeR" Montoro

DEF CON Workshops - cont...(14:00-17:59 PDT) - [Sold Out - Reaching Mythos: Hands-On Vulnerability Discovery with Local AI Models](#) - John "clearbluejar" McIntosh

DEF CON Workshops - cont...(14:00-17:59 PDT) - [Sold Out - Solder, Detect, Listen: Build Your Own EMF Explorer](#) - Darcy "@Drc3p0" Neal

DEF CON Workshops - cont...(14:00-17:59 PDT) - [Sold Out - All About Stoopie InfoStealers: Malware Analysis for Understanding, Custom Coding for True Understanding!](#) - Ryan "@rj_chap" Chapman,Aaron "Ironical" Rosenmund

DEF CON Workshops - cont...(14:00-17:59 PDT) - [Sold Out - Introduction to Malware Analysis](#) - Sam Bowne,Elizabeth Biddlecome,Kaitlyn Handelman,Irvin Lemus

DEF CON Workshops - cont...(14:00-17:59 PDT) - [Sold Out - Embedded Computing Tools for Wireless Hardware Hacking](#) - Joseph Long

Demo Labs - [Phasmid: Deniable Storage for Rubber-Hose Scenarios](#) - Makoto "Mr.Rabbit" Sugita

Demo Labs - [AC Scanner: The Post-Quantum Cryptographic Exposure and CBOM Generator. You Need This!](#) - Anurag Swarnim Yadav,Joseph Wilson

Demo Labs - [BigIron.ai: AI-Assisted Exploration and Security Analysis of Mainframe Systems](#) - Adam "w00tock" Toscher

Demo Labs - [DFMI: Weaponizing MSI Installers for Fileless Code Execution](#) - Anil Celik

Demo Labs - [Reversing F5: Pure-Go Steganography, Live Forensic Cover Recovery, and JPEG Fragility Analysis](#) - Overkilll

Demo Labs - [MailX-Ray: A TSA X-Ray for Emails — Air-Gapped Safe-Read and Quick Triage in an Ephemeral MicroVM](#) - Uğur "uJohn" Can ATASOY

Embedded Systems Village - cont...(10:00-17:59 PDT) - [Embedded - 101 Labs](#) -

Embedded Systems Village - cont...(10:00-17:59 PDT) - [Exploit Bluetooth Low Energy with BLESPlloit and optional ESP32](#) - Slawomir Jasek

Embedded Systems Village - cont...(10:00-17:59 PDT) - [Embedded Systems Village CTF](#) -

Game Hacking Village - cont...(12:00-16:59 PDT) - [Riot Games Vanguard: Pwn to own](#) -

Game Hacking Village - [Chill Zone: Smash \(Project Plus\) Tournament with Prizes](#) -

Game Hacking Village - [Bobba! A Complete History of Habbo Hotel Private Servers from Shockwave to HTML5](#) - InsiderPHD

Hackers.town - [Hackers Trivia](#) - RemoteNemesis,Medus4

Ham Radio Village - cont...(15:30-16:18 PDT) - [Advanced Topics in LoRa Meshes](#) - Eric Escobar

IoT Village - cont...(10:00-17:59 PDT) - [Discover GE Appliances!](#) -

IoT Village - cont...(10:00-17:59 PDT) - [Smart Home in the Matter: Blink, Race, Attack CTF](#) -

IoT Village - cont...(10:00-17:59 PDT) - [Expose Hidden Surveillance in Everyday Tech](#) -

IoT Village - cont...(10:00-17:59 PDT) - [Hands-On Hardware Hacking – From JTAG to Root, Memory Patching Boot Process for Root Access](#) -

IoT Village - cont...(10:00-17:59 PDT) - [Just Hacking Training](#) -

IoT Village - cont...(10:00-17:59 PDT) - [All About UART](#) -

IoT Village - cont...(10:00-17:59 PDT) - Raiders of the Lost Firmware: A Hands-On Workshop in IoT Firmware Archaeology -

IoT Village - cont...(10:00-17:59 PDT) - Cat-astrophic Hacking: Breaking Into Smart Litter Boxes -

IoT Village - cont...(15:45-17:15 PDT) - Wi-Fi Self Defense & Hacker Hunting & For Beginners - Kody Kinzie

La Villa Community - Jackpotting? Bypass de EDR? - Hacking ATM - Arnold Jared Morales Yepez

Lockpick Village - Intro to Lockpicking -

Lonely Hackers Club - cont...(10:00-17:59 PDT) - Lonely Hackers Club - Sticker Swap Table -

Lonely Hackers Club - cont...(10:00-17:59 PDT) - Lonely Hackers Club CTF -

Lonely Hackers Club - cont...(10:00-17:59 PDT) - Lonely Hackers Club - Lockpicking Table -

Lonely Hackers Club - cont...(10:30-16:30 PDT) - Resume Review with the Lonely Hackers Club -

Maker's Village - cont...(10:00-17:59 PDT) - Makers' Village - Hacker Arts and Crafts -

Maker's Village - cont...(15:00-16:59 PDT) - Cyberdeck Build - Sk!tz0

Malware Village - cont...(15:45-16:25 PDT) - Vibe Check: Exploiting Developer Trust from Prompt Injections to Weaponized Repos - Michael Chan

Malware Village - (16:35-17:15 PDT) - You Hold the Helm: Agentic LLM Workflows for Malware Reversing - Asher Davila, Lenin Alevski

Malware Village - cont...(14:10-17:25 PDT) - The Achaean project-Trojan development for noobs - Leigh Gilbert

Middle Easterns & Africans in Cyber Security (MEACS) - Defense in Depth for AI: Launching the AISECA Framework - Amber Bennoui, Karol Piekarski

Misc - cont...(15:30-16:30 PDT) - tAIrot Readings -

Mobile Hacking Community - cont...(10:00-17:59 PDT) - Mobile Hacking - Informal CTF -

Mobile Hacking Community - cont...(10:00-17:59 PDT) - Mobile Hacking Community - Open -

Mobile Hacking Community - Leveraging Frida to Bypass Mobile Application Security Controls - Jarrod Rizor

Nix Vegas Community - NixOS Workspaces - JB

Nix Vegas Community - (16:45-16:59 PDT) - Github Rate Limits Got You Down? FOD's Failing to Build? Let's Talk About Caching - Ethan Carter Edwards

Noob Community - cont...(10:00-17:59 PDT) - Skillbit Labs -

Noob Community - cont...(10:00-17:59 PDT) - TCM Security Labs -

Noob Community - cont...(10:00-17:59 PDT) - SANS Institute NetWars Labs -

Noob Community - cont...(10:00-17:59 PDT) - No Stupid Questions -

Noob Community - cont...(10:00-17:59 PDT) - Hack The Box DC Junior Ranger Program Challenge -

Noob Community - cont...(10:00-17:59 PDT) - Kryptsec Labs -

Noob Community - cont...(10:00-17:59 PDT) - Mentoring and Career Advice -

Noob Community - cont...(10:00-17:59 PDT) - Arcanum Security Labs -

Noob Community - cont...(15:30-16:59 PDT) - Introduction to Web Exploitation - Roman Bohuk

Noob Community - Building Your First Homelab - Stephen Glombicki

Noob Community - (16:35-17:05 PDT) - The Front Lines Need Detection Engineers : Would You Like to Know More? - Kyle Barboza

OSINT For Good Community - cont...(10:00-17:59 PDT) - FINDX OSINT Educational Series -

OSINT For Good Community - cont...(10:00-17:59 PDT) - OSINT4Good Community - DC NextGen Content -

OSINT For Good Community - cont...(15:30-16:30 PDT) - Trace Labs L100: Search Party Basics - Sarah "scba" Miller

OWASP Foundation - cont...(10:00-17:59 PDT) - BadVR: Signals Everywhere a collaboration with XR Village - Jad Meouchy, Suzanne Borders

OWASP Foundation - OWASP Amass v5.0 - Jeff Foley

Payment Village - Breaking BIOS in ATMs - Arnold Jared Morales Yepez

Physical Security Village - The Door Was Already Open - Champ

Policy @ DEF CON - Building a State Wide VDP: Lessons from Maryland's First Year in the Trenches - 01dbae

Policy @ DEF CON - cont...(15:30-16:30 PDT) - Privacy's Defender: How Hackers Protected the Internet Before and Can Do It Again - Cindy Cohn

Policy @ DEF CON - (16:30-16:59 PDT) - Legally Hacked: how countries decide when security research Is allowed - Katharina "Kat S" Sommer

Policy @ DEF CON - cont...(15:30-16:30 PDT) - When AI Finds Everything: Vulnerability Policy for the Coming Discovery Surge - Alec Summers, Lindsey Cerkovnik, Madison Ficorelli

Policy @ DEF CON - (16:30-17:59 PDT) - Filibuffer Overflow: Hackers Stage A Congressional Hearing - Katherine Pratt, Jeff Rothblum, Maurice Turner, Ayan Islam, Beau Woods

Quantum Village - (16:30-16:59 PDT) - [Covert Quantum Computing - a new quantum security paradigm](#) - Evan Anderson

Radio Frequency Village - cont...(10:00-17:59 PDT) - [Radio Frequency Village Events](#) -

Radio Frequency Village - cont...(15:30-16:25 PDT) - [AI-assisted RF Hacking with GNU Radio](#) - Erwin Karincic (Dollarhyde)

Radio Frequency Village - (16:30-16:55 PDT) - [Supertooth: Wideband Bluetooth Observation with a HackRF](#) - Dalton Cox

Radio Frequency Village - [Practical Guidance for RF Researchers: Experiment First, Interfere Never](#) - Andy Hendrickson

Recon Village - cont...(10:00-23:59 PDT) - [Live Recon Contest](#) -

Recon Village - cont...(10:00-23:59 PDT) - [TrackTheFugitive Contest](#) -

Recon Village - cont...(11:00-16:59 PDT) - [GE\(O\)SINT Contest](#) -

Recon Village - cont...(15:30-17:59 PDT) - [BBOT: Automating the OSINT Kill Chain with a Single Command](#) - Mark Gaddy

Recon Village - (16:30-16:59 PDT) - [Groking the Kill Chain](#) - Anthony Russell

Red Team Village - cont...(10:00-17:59 PDT) - [From Kiosk to Domain Compromise: Learning to Walk Up and Take it All](#) - Ezra Woods, Mike Manrod, Spencer Alessi

Red Team Village - cont...(10:00-17:59 PDT) - [BloodHound Quest](#) - Hugo van den Toorn

Red Team Village - [EvilEssid: Evading Wireless Intrusion Prevention Systems](#) - Miguel Fernandez

Red Team Village - [redStack: Boot-To-Breach Red Team Platform](#) - Michael Kim, Michael Ortiz

Red Team Village - [Haetae: An Agent to Takedown North Korean C2 Servers](#) - Mauro Eldritch, Nelson Rafael Colón Merán

Red Team Village - [Praetor: An OPSEC Exposure Advisor for Empire Operators](#) - Andrea Brosio, Ariz Soriano

Red Team Village - [Trust Me, Bro: A field guide to Windows Authenticode Abuse](#) - Fagan Afandiyev

Red Team Village - [Network Implants: Lessons Learned Building Reliable Red Team Dropboxes](#) - Hassan Mohamad

Scambait Village - cont...(10:00-17:59 PDT) - [Open Q&A](#) -

Scambait Village - cont...(10:00-17:59 PDT) - [KSCM Scambait Radio](#) -

Scambait Village - cont...(14:00-17:59 PDT) - [Live Call Listening](#) -

Social Engineering Community Village - cont...(08:30-17:59 PDT) - [Social Engineering Community Village - Open Hours](#) -

Social Engineering Community Village - [Cold Calls](#) -

Social Engineering Community Village - cont...(15:30-16:59 PDT) - [SE Improv](#) - Bryan, Kevin

Social Gatherings/Events - cont...(08:00-18:59 PDT) - [Human Registration Open](#) -

Social Gatherings/Events - cont...(10:00-16:59 PDT) - [Malysis: A Bare-Metal RAM Enclave for Malware Analysis. No Hypervisor. No Trace.](#) - Yannick LaRue, Samuel B. G.

Social Gatherings/Events - cont...(10:00-16:59 PDT) - [Malysis: A Bare-Metal RAM Enclave for Malware Analysis. No Hypervisor. No Trace.](#) - Yannick LaRue, Samuel B. G.

Social Gatherings/Events - cont...(15:00-16:59 PDT) - [Book Signing - Avinash Majeti](#) - Avinash Majeti

Social Gatherings/Events - [Book Signing - Avinash Majeti](#) - Avinash Majeti

Social Gatherings/Events - cont...(08:00-17:59 PDT) - [Merch \(formerly swag\) Area Open -- README](#) -

Social Gatherings/Events - cont...(10:00-18:59 PDT) - [Music - SomaFM](#) -

Social Gatherings/Events - [Queercon Mixer](#) -

Social Gatherings/Events - [Atlanta Metro Meetup \(DC404/DC678/DC770/DC470\)](#) -

Telecom Village - [Nation State Obfuscation Networks](#) - Will Thomas

Telecom Village - (16:30-16:59 PDT) - [Telecom Village CTF Closure](#) -

Voting Village - cont...(10:00-17:59 PDT) - [Voting Village Lab](#) -

Voting Village - [Security and Privacy for the Rest of Elections](#) - Michael Specter

Voting Village - (16:30-16:59 PDT) - [Watching Norway's Election](#) - Hallvard Nygard

[Return to Index](#) - [Locations Legend](#)

[.EDU Community](#) - [.edu Community Mixer](#) -
[Adversary Village](#) - (17:15-17:59 PDT) - [Where hackers find their people, and security finds its strength](#) - Seeyew Mo,Ashley S,Tatiana U,Heidi Potter,Christine Billingsley
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Drone Hacking Choose your Own Adventure](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Drone Hacking Workshop](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [MOUSE Runner & Flappy Drone](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Flight Simulator/EFB](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Satellites Under Attack: Hands-On Satellite Security Threat Scenarios](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [SpaceCOP - Catch Me If You Can](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Nebula Showdown: Space Systems Security CTF Adventure](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [SR-71 Blackbird Badge Challenge](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Mission: Compromised - Hacking a Satellite from the Ground Up](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [ARINC 664 CTF Challenge](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Aerospace Ecosystem Resilience Innovation Environment \(AERIE\) Cyber Range](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [DCNextGen - RIC-1: ELT Localization Exercise - N3VR-G0N Down](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Bricks in the Air](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Aviation ISAC Cybersecurity Challenge](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [DCNextGen - Bricks in the Air](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [DCNextGen - Space Grand Challenge - SatHack: The MOUSE-1 Mission](#) -
[AI Village](#) - cont...(10:00-17:59 PDT) - [AI Village: Village Open](#) -
[AI Village](#) - cont...(10:00-17:59 PDT) - [Poster Presentations](#) -
[AI Village](#) - cont...(10:00-17:59 PDT) - [Cyber Mirage: Realtime Deepfake Demos](#) - Brandon Kovacs
[AppSec Village](#) - cont...(16:30-17:30 PDT) - [Rebuilding Code Security with Signal, Speed and AI](#) - Derek C.,Shasheen Bandodkar
[AppSec Village](#) - cont...(16:50-17:20 PDT) - [Most threat modeling artifacts don't help coding agents fix business logic. Here's what does.](#) - Meitar Ronen
[AppSec Village](#) - (17:30-17:59 PDT) - [Trust No History: Why Every "Remembered" Interaction is a Potential Backdoor](#) - Barno Kaharova,Rico Komenda
[Biohacking Village](#) - cont...(10:00-17:59 PDT) - [Embedded & Shredded: Advanced Embedded System Hacking](#) -
[Biohacking Village](#) - cont...(10:00-17:59 PDT) - [Biohacking Device Lab](#) -
[Biohacking Village](#) - (17:30-17:59 PDT) - [Hacking Hearts by Reverse Engineering Pacemaker Firmware](#) - Marie Moe,Shayan Alinejad,Kristian Karlsen
[Biohacking Village](#) - cont...(16:30-17:15 PDT) - [Lights Out and Last Call: A Drunken Tabletop on Medical Device Resilience](#) - Courtney McCarty
[Blacks In Cyber Village](#) - cont...(16:00-17:30 PDT) - [KaliGPT Vibe-Ethical Hacking Session](#) - Timothy E. Bates
[Blue Team Village](#) - [Cloudy with a Chance of Venting: Managing Supply Chain Risk](#) - Cassandra (muteki) Young,Christian Nicholson,David Collins,Kyle Dickinson,Ricky (Oxpsilocyber) Banda
[Bug Bounty Village](#) - [Beyond Normalization: The Expanding Unicode Attack Surface](#) - Ryan "ryancbarnett" Barnett,Isabella "4ng3lhacker" Barnett
[Call Center Village](#) - cont...(10:00-17:59 PDT) - [Call Center Village - Open](#) -
[Car Hacking Village](#) - cont...(10:00-17:59 PDT) - [Car Hacking Village Open](#) -
[Cloud Village](#) - cont...(16:00-17:59 PDT) - [Cirro: Extending Your Azure Graph Beyond Identities](#) - Leron Gray
[Cloud Village](#) - cont...(16:00-17:59 PDT) - [From Dashboard to Exploit: Weaponizing and Winning the Cloud Queue](#) - Mackenzie Jackson
[Cloud Village](#) - cont...(16:50-17:30 PDT) - [Trust Fall: How Agentic AI Inherits Your Cloud's Worst IAM Habits](#) - Aravind Sreekanth Pallavoor,Sadhana Sainarayanan
[CodeBloom](#) - [Work Session: Binary Code](#) -
[Contests](#) - cont...(16:00-17:59 PDT) - [Um, ACKtually](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [5N4CK3Y](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [DC's Next Top Threat Model](#) -

[Contests](#) - cont...(10:00-17:59 PDT) - [Untechnical](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [DEF CON Scavenger Hunt](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Darknet-NG](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Crack Me If You Can 2026](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [TeleChallenge](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [HackFortress](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [?Cube](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [\\$unLight Sh4d0w5](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Octopus Game - Booth Open](#) -
[Contests](#) - [Octopus Game - Booth Battle #2: The Midnight "Brawl"](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Beer Chilling Contraption Contest](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Cryptid Hunt](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [HSPACE: AI Battlegrounds](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [spyVspy 3: Rat Race](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Hacker Games](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [PhreakMe](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Game Hacking Village CTF](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Kubernetes CTF](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Hac-Man](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Crack the Core](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Cyber Deck Competition](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Pinball High Score Contest](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Code Cadaver: Break Every System. Save Your Friend.](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [PWN UR H0M3 - DDoS CTF](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Real7y Overrun - Contest running](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Tin Foil Hat Contest](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [CMD+CTRL Cyber Range: DarkMoney](#) -
[Contests](#) - cont...(13:00-17:59 PDT) - [Locktopus - Open Qualifying](#) -
[Contests](#) - cont...(11:00-17:59 PDT) - [Radio Frequency Capture the Flag](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [DEF CON CTF: Benevolent Bureau of Birds](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [AI Village - Hal CTF](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [AI Village Plays Pokemon: DEFCON Edition](#) - Nick Ashworth
[Contests](#) - cont...(10:00-17:59 PDT) - [OWASP CTF](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Escalation Desk CTF](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [DEF CON Groups Sticker Contest](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [DEF CON Groups Backdoors & Breaches](#) - Tim Doerges, Seth Benning
[Contests](#) - cont...(10:00-23:59 PDT) - [Apex Park \(Cloud Village CTF\)](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Hacking GRC Contest](#) -
[Crypto & Privacy Village](#) - cont...(16:30-17:15 PDT) - [Crypto Is Fine. The Code Is Not: Real-World Cryptographic Failures](#) -
Diptendu Kar
[Crypto & Privacy Village](#) - (17:15-17:59 PDT) - [2026 is the New 2016: Relearning the Lessons from the "Year of the Data Breach"](#) - Anthony Hendricks
[Cryptocurrency Village](#) - [Blockchain defense, stablecoin attacks, and Web3 OSINT](#) - Dinmukhammed "Celestial"
Kabiden, Izdihar, KL4R10N
[Data Duplication Village](#) - cont...(10:00-17:59 PDT) - [DDV open and accepting drives for duplication](#) -
[DCNextGen](#) - [Welcome to your Airbnb, the key is under the mat -or- Alice and Bob with Padlocks](#) - Gilgamesh
[DEF CON Groups](#) - cont...(10:00-17:59 PDT) - [DEF CON Groups \(DCG\)](#) -
[DEF CON Talks](#) - [Hacking AI](#) - Bruce Schneier
[DEF CON Talks](#) - cont...(16:30-17:30 PDT) - [noRecognition: Could a pattern on your clothing fool Facial Facial Recognition?](#) - Bill "hevnsnt" Swearingen
[DEF CON Talks](#) - (17:30-17:59 PDT) - [Breaking Hardware CFI with Sigreturn](#) - Omri "beta_b0t" Ben Bassat
[DEF CON Talks](#) - [One Chain to Own Them All — Breaking AI Infrastructures](#) - Ji'an "azraelxuemo" Zhou, Lei "llfamsec" Lu
[DEF CON Talks](#) - cont...(16:30-17:30 PDT) - [CloudBashing: Exploiting free CloudShells for mining, networking, exfil, and persistence at scale](#) - Jenko "edleft" Hwong, Chris Ryan
[DEF CON Talks](#) - (17:30-17:59 PDT) - [You've Got Mail \(That Was Meant For No One\)](#) - Cøry "interpunkt" Solovewicz

DEF CON Talks - Gotta Catch 'Em All: How To Capture 3.5 Billion WhatsApp Accounts - Maximilian Guenther,Gabriel Gegenhuber

DEF CON Training - cont...(08:30-17:30 PDT) - Beat the Breach: Defend, Respond, Survive - McKay Hardy,Wes Wagstaff

DEF CON Training - cont...(08:30-17:30 PDT) - Cyber & AI Policy Basics: What Every Organization Needs in Place - Pamela 'Pam' Feld,Greg Goldberg

DEF CON Training - cont...(08:30-17:30 PDT) - Digital Supply Chain Security: Software, Cryptography, AI, and Vendor Risk - Anant Shrivastava,Sunil Yadav

DEF CON Workshops - cont...(14:00-17:59 PDT) - Sold Out - Investigating and Responding to M365 account compromise on a shoestring: Living of the Land Incident Response - Vince "bitpusher" Weppner

DEF CON Workshops - cont...(14:00-17:59 PDT) - Sold Out - OT Systems: how to secure them in practice! - Alexandrine Torrents,Arnaud SOULLIE

DEF CON Workshops - cont...(14:00-17:59 PDT) - Sold Out - AWS Principal Threat Hunting: Behavioral Baselining for Malicious Activity - Rodrigo "Sp0oKeR" Montoro

DEF CON Workshops - cont...(14:00-17:59 PDT) - Sold Out - Reaching Mythos: Hands-On Vulnerability Discovery with Local AI Models - John "clearbluejar" McIntosh

DEF CON Workshops - cont...(14:00-17:59 PDT) - Sold Out - Solder, Detect, Listen: Build Your Own EMF Explorer - Darcy "@Drc3p0" Neal

DEF CON Workshops - cont...(14:00-17:59 PDT) - Sold Out - All About Stoopie InfoStealers: Malware Analysis for Understanding, Custom Coding for True Understanding! - Ryan "@rj_chap" Chapman,Aaron "Ironical" Rosenmund

DEF CON Workshops - cont...(14:00-17:59 PDT) - Sold Out - Introduction to Malware Analysis - Sam Bowne,Elizabeth Biddlecome,Kaitlyn Handelman,Irvin Lemus

DEF CON Workshops - cont...(14:00-17:59 PDT) - Sold Out - Embedded Computing Tools for Wireless Hardware Hacking - Joseph Long

Embedded Systems Village - cont...(10:00-17:59 PDT) - Embedded - 101 Labs -

Embedded Systems Village - cont...(10:00-17:59 PDT) - Exploit Bluetooth Low Energy with BLESPlloit and optional ESP32 - Slawomir Jasek

Embedded Systems Village - cont...(10:00-17:59 PDT) - Embedded Systems Village CTF -

ICS Village - Lessons Learned from Poland and Beyond: The State of Electric Sector Attacks in 2025 - Joe Slowik

ICS Village - (17:30-17:59 PDT) - Exposed Data Centers: Bypass IT Security, Crank Up the Heat - Stephen Hilt,Numaan Huq

IoT Village - cont...(10:00-17:59 PDT) - Hands-On Hardware Hacking – From JTAG to Root, Memory Patching Boot Process for Root Access -

IoT Village - cont...(10:00-17:59 PDT) - Just Hacking Training -

IoT Village - cont...(10:00-17:59 PDT) - All About UART -

IoT Village - cont...(10:00-17:59 PDT) - Raiders of the Lost Firmware: A Hands-On Workshop in IoT Firmware Archaeology -

IoT Village - cont...(10:00-17:59 PDT) - Cat-astrophic Hacking: Breaking Into Smart Litter Boxes -

IoT Village - cont...(10:00-17:59 PDT) - Smart Home in the Matter: Blink, Race, Attack CTF -

IoT Village - cont...(10:00-17:59 PDT) - Discover GE Appliances! -

IoT Village - cont...(10:00-17:59 PDT) - Expose Hidden Surveillance in Everyday Tech -

IoT Village - cont...(15:45-17:15 PDT) - Wi-Fi Self Defense & Hacker Hunting & For Beginners - Kody Kinzie

La Villa Community - Tokens and PRT: Advanced Attacks and Persistence in Microsoft Entra ID - Elzer Pineda,Jose Rivas

Lonely Hackers Club - cont...(10:00-17:59 PDT) - Lonely Hackers Club - Sticker Swap Table -

Lonely Hackers Club - cont...(10:00-17:59 PDT) - Lonely Hackers Club - Lockpicking Table -

Lonely Hackers Club - cont...(10:00-17:59 PDT) - Lonely Hackers Club CTF -

Maker's Village - cont...(10:00-17:59 PDT) - Makers' Village - Hacker Arts and Crafts -

Malware Village - cont...(16:35-17:15 PDT) - You Hold the Helm: Agentic LLM Workflows for Malware Reversing - Asher Davila,Lenin Alevski

Malware Village - cont...(14:10-17:25 PDT) - The Achaean project-Trojan development for noobs - Leigh Gilbert

Middle Easterns & Africans in Cyber Security (MEACS) - Condense, Contextualize, and Correlate: Optimize Costs while Connecting the Dots at Scale - Ezz Tahoun

Middle Easterns & Africans in Cyber Security (MEACS) - What Got You Here Won't Get You There: Security in the AI Era - Amber Bennoui

Mobile Hacking Community - cont...(10:00-17:59 PDT) - Mobile Hacking Community - Open -

Mobile Hacking Community - cont...(10:00-17:59 PDT) - Mobile Hacking - Informal CTF -

Nix Vegas Community - Lightning Talks and Unconference -

[Noob Community](#) - cont...(10:00-17:59 PDT) - [SANS Institute NetWars Labs](#) -
[Noob Community](#) - cont...(10:00-17:59 PDT) - [TCM Security Labs](#) -
[Noob Community](#) - cont...(10:00-17:59 PDT) - [Skillbit Labs](#) -
[Noob Community](#) - cont...(10:00-17:59 PDT) - [Mentoring and Career Advice](#) -
[Noob Community](#) - cont...(10:00-17:59 PDT) - [Hack The Box DC Junior Ranger Program Challenge](#) -
[Noob Community](#) - cont...(10:00-17:59 PDT) - [Arcanum Security Labs](#) -
[Noob Community](#) - cont...(10:00-17:59 PDT) - [No Stupid Questions](#) -
[Noob Community](#) - cont...(10:00-17:59 PDT) - [Kryptsec Labs](#) -
[Noob Community](#) - cont...(16:35-17:05 PDT) - [The Front Lines Need Detection Engineers : Would You Like to Know More?](#)
 - Kyle Barboza
[OSINT For Good Community](#) - cont...(10:00-17:59 PDT) - [FINDX OSINT Educational Series](#) -
[OSINT For Good Community](#) - cont...(10:00-17:59 PDT) - [OSINT4Good Community - DC NextGen Content](#) -
[OSINT For Good Community](#) - (17:30-17:59 PDT) - [Tracelabs VM Installation Workshop](#) -
[OSINT For Good Community](#) - [Installing and Using the Tracelabs VM](#) - Jeff "UltraSunshine" G
[OWASP Foundation](#) - (17:30-17:59 PDT) - [AI Pentesting is not a Vibe Check](#) - Ads Dawson
[OWASP Foundation](#) - cont...(10:00-17:59 PDT) - [BadVR: Signals Everywhere a collaboration with XR Village](#) - Jad
 Meouchy,Suzanne Borders
[OWASP Foundation](#) - cont...(16:00-17:59 PDT) - [OWASP Amass v5.0](#) - Jeff Foley
[Policy @ DEF CON](#) - cont...(16:30-17:59 PDT) - [Filibuffer Overflow: Hackers Stage A Congressional Hearing](#) - Katherine
 Pratt,Jeff Rothblum,Maurice Turner,Ayan Islam,Beau Woods
[Quantum Village](#) - [Q-Day - the Early Years...](#) - Konstantinos Karagiannis
[Radio Frequency Village](#) - cont...(10:00-17:59 PDT) - [Radio Frequency Village Events](#) -
[Radio Frequency Village](#) - [WiFi Shuriken: A New Architecture For High Performance Scanning](#) - CoD_Segfault
[Radio Frequency Village](#) - [Latest News in the Proxmark World](#) - Iceman
[Recon Village](#) - cont...(10:00-23:59 PDT) - [TrackTheFugitive Contest](#) -
[Recon Village](#) - cont...(10:00-23:59 PDT) - [Live Recon Contest](#) -
[Recon Village](#) - cont...(15:30-17:59 PDT) - [BBOT: Automating the OSINT Kill Chain with a Single Command](#) - Mark Gaddy
[Red Team Village](#) - cont...(10:00-17:59 PDT) - [From Kiosk to Domain Compromise: Learning to Walk Up and Take it All](#) -
 Ezra Woods,Mike Manrod,Spencer Alessi
[Red Team Village](#) - cont...(10:00-17:59 PDT) - [BloodHound Quest](#) - Hugo van den Toorn
[Red Team Village](#) - cont...(16:00-17:59 PDT) - [EvilEssid: Evading Wireless Intrusion Prevention Systems](#) - Miguel Fernandez
[Red Team Village](#) - cont...(16:00-17:59 PDT) - [redStack: Boot-To-Breach Red Team Platform](#) - Michael Kim,Michael Ortiz
[Red Team Village](#) - cont...(16:00-17:59 PDT) - [Haetae: An Agent to Takedown North Korean C2 Servers](#) - Mauro
 Eldritch,Nelson Rafael Colón Merán
[Red Team Village](#) - cont...(16:00-17:59 PDT) - [Praetor: An OPSEC Exposure Advisor for Empire Operators](#) - Andrea
 Brosio,Ariz Soriano
[Scambait Village](#) - cont...(10:00-17:59 PDT) - [Open Q&A](#) -
[Scambait Village](#) - cont...(10:00-17:59 PDT) - [KSCM Scambait Radio](#) -
[Scambait Village](#) - cont...(14:00-17:59 PDT) - [Live Call Listening](#) -
[Social Engineering Community Village](#) - cont...(08:30-17:59 PDT) - [Social Engineering Community Village - Open Hours](#) -
[Social Engineering Community Village](#) - cont...(16:00-17:59 PDT) - [Cold Calls](#) -
[Social Gatherings/Events](#) - cont...(08:00-18:59 PDT) - [Human Registration Open](#) -
[Social Gatherings/Events](#) - cont...(08:00-17:59 PDT) - [Merch \(formerly swag\) Area Open -- README](#) -
[Social Gatherings/Events](#) - cont...(10:00-18:59 PDT) - [Music - SomaFM](#) -
[Social Gatherings/Events](#) - [Friends of Bill W](#) -
[Social Gatherings/Events](#) - cont...(16:00-17:59 PDT) - [Queercon Mixer](#) -
[Social Gatherings/Events](#) - cont...(16:00-18:59 PDT) - [Atlanta Metro Meetup \(DC404/DC678/DC770/DC470\)](#) -
[Telecom Village](#) - [Telecom Village Open Forum: Talks & Workshops: Review, Highlights, and Key Learnings](#) -
[The Diana Initiative](#) - [Yoga](#) - Deanna Heon
[Voting Village](#) - cont...(10:00-17:59 PDT) - [Voting Village Lab](#) -
[Voting Village](#) - [We Pwn Your Phone, We Pwn Your Vote \(Demo and Panel\)](#) - Brian DeMuth,Matt Blaze,David
 Jefferson,Michael Specter

Friday - 18:00 PDT

[Return to Index](#) - [Locations Legend](#)

[Contests](#) - cont...(10:00-23:59 PDT) - [Apex Park \(Cloud Village CTF\)](#) -
[Recon Village](#) - cont...(10:00-23:59 PDT) - [Live Recon Contest](#) -
[Recon Village](#) - cont...(10:00-23:59 PDT) - [TrackTheFugitive Contest](#) -
[Social Gatherings/Events](#) - cont...(08:00-18:59 PDT) - [Human Registration Open](#) -
[Social Gatherings/Events](#) - cont...(10:00-18:59 PDT) - [Music - SomaFM](#) -
[Social Gatherings/Events](#) - (18:30-20:30 PDT) - [Policy Mixer Happy Hour](#) -
[Social Gatherings/Events](#) - [Exploit Your Own Story](#) - Charel "1C0nur3r" Morris
[Social Gatherings/Events](#) - cont...(16:00-18:59 PDT) - [Atlanta Metro Meetup \(DC404/DC678/DC770/DC470\)](#) -

Friday - 19:00 PDT

[Return to Index](#) - [Locations Legend](#)

[Contests](#) - [AI Art Battle](#) -

[Contests](#) - cont...(10:00-23:59 PDT) - [Apex Park \(Cloud Village CTF\)](#) -

[Recon Village](#) - cont...(10:00-23:59 PDT) - [Live Recon Contest](#) -

[Recon Village](#) - cont...(10:00-23:59 PDT) - [TrackTheFugitive Contest](#) -

[Social Gatherings/Events](#) - [Music - Genre: Goth / Industrial](#) - [Daemon Chadeau](#)

[Social Gatherings/Events](#) - cont...(18:30-20:30 PDT) - [Policy Mixer Happy Hour](#) -

[Social Gatherings/Events](#) - [BlanketFort Con](#) -

[Social Gatherings/Events](#) - [Lawyers Meet](#) -

[Social Gatherings/Events](#) - cont...(18:00-19:59 PDT) - [Exploit Your Own Story](#) - [Charel "IC0nur3r" Morris](#)

[Social Gatherings/Events](#) - [Social Engineering Community Village Party](#) -

[Social Gatherings/Events](#) - [The KEVOPS Sellout Pool Party II: Sponsored by Zyn](#) -

Friday - 20:00 PDT

[Return to Index](#) - [Locations Legend](#)

[Contests](#) - cont...(19:00-20:59 PDT) - [AI Art Battle](#) -
[Contests](#) - cont...(10:00-23:59 PDT) - [Apex Park \(Cloud Village CTF\)](#) -
[Recon Village](#) - cont...(10:00-23:59 PDT) - [TrackTheFugitive Contest](#) -
[Recon Village](#) - cont...(10:00-23:59 PDT) - [Live Recon Contest](#) -
[Social Gatherings/Events](#) - [Hacker Jeopardy](#) -
[Social Gatherings/Events](#) - [Music - Genre: Goth / Industrial](#) - DJ Scythe
[Social Gatherings/Events](#) - [Women, gender non-conforming and non-binary meetup with The Diana Initiative](#) -
[Social Gatherings/Events](#) - cont...(18:30-20:30 PDT) - [Policy Mixer Happy Hour](#) -
[Social Gatherings/Events](#) - [Movie Night](#) -
[Social Gatherings/Events](#) - [Hacker Karaoke](#) -
[Social Gatherings/Events](#) - cont...(19:00-21:59 PDT) - [Lawyers Meet](#) -
[Social Gatherings/Events](#) - cont...(19:00-22:59 PDT) - [Social Engineering Community Village Party](#) -
[Social Gatherings/Events](#) - cont...(19:00-21:59 PDT) - [The KEVOPS Sellout Pool Party II: Sponsored by Zyn](#) -

Friday - 21:00 PDT

[Return to Index](#) - [Locations Legend](#)

[Contests](#) - [cont...\(10:00-23:59 PDT\)](#) - [Apex Park \(Cloud Village CTF\)](#) -
[Recon Village](#) - [cont...\(10:00-23:59 PDT\)](#) - [TrackTheFugitive Contest](#) -
[Recon Village](#) - [cont...\(10:00-23:59 PDT\)](#) - [Live Recon Contest](#) -
[Social Gatherings/Events](#) - [cont...\(20:00-21:59 PDT\)](#) - [Hacker Jeopardy](#) -
[Social Gatherings/Events](#) - [Arcade Party](#) -
[Social Gatherings/Events](#) - [Music - Genre: Nerdcore](#) - [Ohm-I](#)
[Social Gatherings/Events](#) - [cont...\(20:00-23:30 PDT\)](#) - [Women, gender non-conforming and non-binary meetup with The Diana Initiative](#) -
[Social Gatherings/Events](#) - [cont...\(20:00-23:59 PDT\)](#) - [Movie Night](#) -
[Social Gatherings/Events](#) - [cont...\(19:00-21:59 PDT\)](#) - [Lawyers Meet](#) -
[Social Gatherings/Events](#) - [cont...\(19:00-22:59 PDT\)](#) - [Social Engineering Community Village Party](#) -
[Social Gatherings/Events](#) - [BIC R00T ACCESS 2026](#) -
[Social Gatherings/Events](#) - [Day of the Dead Hacker Party](#) -
[Social Gatherings/Events](#) - [cont...\(19:00-21:59 PDT\)](#) - [The KEVOPS Sellout Pool Party II: Sponsored by Zyn](#) -

Friday - 22:00 PDT

[Return to Index](#) - [Locations Legend](#)

[Contests](#) - cont...(10:00-23:59 PDT) - [Apex Park \(Cloud Village CTF\)](#) -
[Recon Village](#) - cont...(10:00-23:59 PDT) - [Live Recon Contest](#) -
[Recon Village](#) - cont...(10:00-23:59 PDT) - [TrackTheFugitive Contest](#) -
[Social Gatherings/Events](#) - [Whose Slide Is It Anyway?](#) -
[Social Gatherings/Events](#) - [SecKC the WHOLE WIDE WORLD](#) -
[Social Gatherings/Events](#) - [Music](#) - Genre: [House](#) - [Skittish & Bus](#)
[Social Gatherings/Events](#) - cont...(20:00-23:30 PDT) - [Women, gender non-conforming and non-binary meetup with The Diana Initiative](#) -
[Social Gatherings/Events](#) - [Slopcon](#) -
[Social Gatherings/Events](#) - cont...(20:00-23:59 PDT) - [Movie Night](#) -
[Social Gatherings/Events](#) - cont...(19:00-22:59 PDT) - [Social Engineering Community Village Party](#) -

Friday - 23:00 PDT

[Return to Index](#) - [Locations Legend](#)

[Contests](#) - cont...(10:00-23:59 PDT) - [Apex Park \(Cloud Village CTF\)](#) -

[Recon Village](#) - cont...(10:00-23:59 PDT) - [TrackTheFugitive Contest](#) -

[Recon Village](#) - cont...(10:00-23:59 PDT) - [Live Recon Contest](#) -

[Social Gatherings/Events](#) - cont...(22:00-23:59 PDT) - [Whose Slide Is It Anyway?](#) -

[Social Gatherings/Events](#) - [Music](#) - [Genre: Techno](#) - [TRIODE](#)

[Social Gatherings/Events](#) - cont...(20:00-23:30 PDT) - [Women, gender non-conforming and non-binary meetup with The Diana Initiative](#) -

[Social Gatherings/Events](#) - cont...(20:00-23:59 PDT) - [Movie Night](#) -

Saturday

This Schedule is tentative and may be changed at any time. Check [here](#), [Hacker Tracker](#), or the nearest NFO Node for the latest.

Saturday - 00:00 PDT

[Return to Index](#) - [Locations Legend](#)

[Social Gatherings/Events](#) - [Music](#) - [Genre: Trance](#) - [AfterGlow](#)

[Return to Index](#) - [Locations Legend](#)

[DEF CON Training](#) - (08:30-17:30 PDT) - [Blue vs Red Bootcamp: From Attacker Playbooks to Defender Detections](#) - Carlo Anez Mazurco,Mariana Ruiz

[DEF CON Training](#) - (08:30-17:30 PDT) - [Influence Operations: Tactics, Defense, and Exploitation](#) - Greg Conti,Tom Cross

[DEF CON Training](#) - (08:30-17:30 PDT) - [Full-Stack Pentesting Laboratory: 100% Hands-On + Lifetime LAB Access](#) - Dawid Czagan

[Return to Index](#) - [Locations Legend](#)

[DEF CON Training](#) - cont...(08:30-17:30 PDT) - [Blue vs Red Bootcamp: From Attacker Playbooks to Defender Detections](#) - Carlo Anez Mazurco,Mariana Ruiz

[DEF CON Training](#) - cont...(08:30-17:30 PDT) - [Influence Operations: Tactics, Defense, and Exploitation](#) - Greg Conti,Tom Cross

[DEF CON Training](#) - cont...(08:30-17:30 PDT) - [Full-Stack Pentesting Laboratory: 100% Hands-On + Lifetime LAB Access](#) - Dawid Czagan

[DEF CON Workshops](#) - [Sold Out](#) - [Wi-Fight Club: I am Jack's Evil Twin](#) - James Hawk,Jon "C4V3M4N" Milkins,Brian Burnett

[DEF CON Workshops](#) - [Sold Out](#) - [Explore the Windows instrumentation callback](#) - Yoann "OtterHacker" DEQUEKER

[DEF CON Workshops](#) - [Sold Out](#) - [Step-by-Step Malware Development: Evading EDR from Loaders to the Kernel](#) - Yu Terada,Kotaro "@Decamark / @BinaryPoodle" Osugi

[DEF CON Workshops](#) - [Sold Out](#) - [Words As Weapons: Breaking AI and Agents; Then Securing Them](#) - Pavan "pavanreddysec" Reddy

[DEF CON Workshops](#) - [Sold Out](#) - [HackTheCloud26: Chaining Cloud Misconfigurations to Compromise Infrastructure](#) - HackeMate

[DEF CON Workshops](#) - [Sold Out](#) - [Hecate: A Trivial UART Tool](#) - mx,Joe "SecurelyFitz" FitzPatrick,nyx

[DEF CON Workshops](#) - [Sold Out](#) - [Detecting and Analyzing Memory Only Malware with Volatility 3](#) - Andrew Case,Pierre "Abyss Watcher" Breton,David McDonald

[DEF CON Workshops](#) - [Sold Out](#) - [Battle-Tested Broadcasts: RF Insights From Ukraine](#) - Preston Zen

[Social Gatherings/Events](#) - [Human Registration Open](#) -

[Social Gatherings/Events](#) - [Merch \(formerly swag\) Area Open -- README](#) -

[Return to Index](#) - [Locations Legend](#)

[Adversary Village](#) - [MCPwned: How Exposed AI Agents Became the Internet's New Recon Toy](#) - Eli Woodward

[Adversary Village](#) - (10:30-10:59 PDT) - [Emulating the "Identity-First" Threat Actor: Automated Playbooks for IdP Hijacking](#) - Samet Can Tasci,Mehmet Önder Key

[Aerospace Village](#) - [DCNextGen](#) - [Bricks in the Air](#) -

[Aerospace Village](#) - [Bricks in the Air](#) -

[Aerospace Village](#) - [DCNextGen](#) - [Space Grand Challenge](#) - [SatHack: The MOUSE-1 Mission](#) -

[Aerospace Village](#) - [DCNextGen](#) - [RIC-1: ELT Localization Exercise](#) - [N3VR-G0N Down](#) -

[Aerospace Village](#) - [ARINC 664 CTF Challenge](#) -

[Aerospace Village](#) - [Aviation ISAC Cybersecurity Challenge](#) -

[Aerospace Village](#) - [Aerospace Ecosystem Resilience Innovation Environment \(AERIE\) Cyber Range](#) -

[Aerospace Village](#) - [SpaceCOP](#) - [Catch Me If You Can](#) -

[Aerospace Village](#) - [Nebula Showdown: Space Systems Security CTF Adventure](#) -

[Aerospace Village](#) - [SR-71 Blackbird Badge Challenge](#) -

[Aerospace Village](#) - [Satellites Under Attack: Hands-On Satellite Security Threat Scenarios](#) -

[Aerospace Village](#) - [Drone Hacking Workshop](#) -

[Aerospace Village](#) - [Drone Hacking Choose your Own Adventure](#) -

[Aerospace Village](#) - [MOUSE Runner & Flappy Drone](#) -

[Aerospace Village](#) - [Mission: Compromised - Hacking a Satellite from the Ground Up](#) -

[Aerospace Village](#) - [Flight Simulator/EFB](#) -

[AI Village](#) - [Poster Presentations](#) -

[AI Village](#) - [Cyber Mirage: Realtime Deepfake Demos](#) - Brandon Kovacs

[AI Village](#) - [AI Village: Village Open](#) -

[AppSec Village](#) - (10:15-11:15 PDT) - [In Untrust We Can Trust: Enforcing Trust Boundaries for Humans and AI Alike](#) - Yariv Tal

[AppSec Village](#) - (10:15-12:59 PDT) - [Prompt Injection: Attacking and Defending AI-Powered Applications](#) - Mohammed Ilyas Ahmed

[AppSec Village](#) - (10:30-10:59 PDT) - [Building Hackbots](#) - Jason "jhaddix" Haddix

[Biohacking Village](#) - [Embedded & Shredded: Advanced Embedded System Hacking](#) -

[Biohacking Village](#) - [Biohacking Device Lab](#) -

[Biohacking Village](#) - [To Catch a Pseudoscientist](#) - James Utley PhD

[Biohacking Village](#) - (10:30-10:59 PDT) - [The Death of Dicom](#) - Michael "v3ga" Aguilar

[Blacks In Cyber Village](#) - [Being Black While Hacking: The Unofficial Survival Guide](#) - Dr. Louis DeWeaver III

[Blue Team Village](#) - [AI for Defenders 101](#) - Anirudh Pratap Singh,Neha Gautam,Omenscan ~

[Bug Bounty Village](#) - [Shadow Webhooks: Hunting for Dangling Event Listeners in Enterprise Workspaces](#) - Samet Can Tasci,Mehmet Önder Key

[Bug Bounty Village](#) - (10:30-10:59 PDT) - [Testing API Business Logic With AI Agents: What We Got Wrong First](#) - Samantha Pearlstein

[Bug Bounty Village](#) - [Turning Recon Coverage into Bug Bounty Signal](#) - Radu Stefan Voloaga

[Bug Bounty Village](#) - (10:45-11:30 PDT) - [You're Invited to Get Hacked: Real-World Exploits in Modern Invitation Systems](#) - Ali "logic-breaker" Kabeel

[Call Center Village](#) - [Call Center Village](#) - [Open](#) -

[Car Hacking Village](#) - [Car Hacking Village Open](#) -

[Car Hacking Village](#) - [Bomb Bot Challenge](#) -

[Cloud Village](#) - [Bashing CloudShells for mining, networking, exfil and persistence at scale](#) - Jenko "edleft" Hwong,Chris Ryan

[Cloud Village](#) - (10:40-11:20 PDT) - [Ghost Records: Automating Dangling DNS & Subdomain Takeover Detection at Enterprise Scale](#) - Jai Kumar Sharma,Tom McCarthy

[CodeBloom](#) - [Game Time: Loops](#) -

[Contests](#) - [Hack3r Runw@y v8.0](#) -

[Contests](#) - [5N4CK3Y](#) -

[Contests](#) - [DC's Next Top Threat Model](#) -

Contests - Untechnical -
Contests - DEF CON Scavenger Hunt -
Contests - Darknet-NG -
Contests - Crack Me If You Can 2026 -
Contests - TeleChallenge -
Contests - HackFortress -
Contests - ?Cube -
Contests - \$unLight Sh4d0w5 -
Contests - Octopus Game - Booth Open -
Contests - Beer Chilling Contraption Contest -
Contests - Cryptid Hunt -
Contests - HSPACE: AI Battlegrounds -
Contests - spyVspy 3: Rat Race -
Contests - Hacker Games -
Contests - PhreakMe -
Contests - Game Hacking Village CTF -
Contests - Kubernetes CTF -
Contests - Hac-Man -
Contests - Crack the Core -
Contests - Cyber Deck Competition -
Contests - Pinball High Score Contest -
Contests - Code Cadaver: Break Every System. Save Your Friend. -
Contests - PWN UR H0M3 - DDoS CTF -
Contests - Reali7y Overrun - Contest running -
Contests - Tin Foil Hat Contest -
Contests - CMD+CTRL Cyber Range: DarkMoney -
Contests - Radio Frequency Capture the Flag -
Contests - DEF CON CTF: Benevolent Bureau of Birds -
Contests - AI Village Plays Pokemon: DEFCON Edition - Nick Ashworth
Contests - AI Village - Hal CTF -
Contests - StarPWN CTF -
Contests - Car Hacking Village CTF -
Contests - OWASP CTF -
Contests - Blue Team Village CTF - Project Obsidian -
Contests - Escalation Desk CTF -
Contests - DEF CON Groups Sticker Contest -
Contests - DEF CON Groups Backdoors & Breaches - Tim Doerges,Seth Benning
Contests - Apex Park (Cloud Village CTF) -
Contests - Hacking GRC Contest -
Contests - Bug Bounty Village CTF - Open -
Cryptocurrency Village - Web3 Security: Hacks, Scams, and Exploits - Philip "AlephNull" Werlau,Kennashka DeSilva
Data Duplication Village - DDV open and accepting drives for duplication -
DCNextGen - Intro to Scratch - N3rd H3Rder
DEF CON Groups - DEF CON Groups (DCG) -
DEF CON Talks - Car Hacking Village Scavenger Hunt Contest -
DEF CON Talks - The Ghost Key: Illusions of "Time Management" in TTLock Smart Locks - Yang Liu,Zhenghan Wang
DEF CON Talks - Memory Laundering via Metal: What EDR Can't See on Your Mac - Hxr1
DEF CON Talks - (10:30-11:30 PDT) - Harvest Now, Decrypt Later: Practical Attacks on Post-Quantum Cryptography
Implementations - Aleksandr Krasnov
DEF CON Talks - From Wind Farm to CHP Plant: The Untold Story of Lateral Movement in a Polish Energy Sector Attack -
Marcin Dudek
DEF CON Talks - No Socket, No Privs, No Problem: Weaponizing OCI Registries for SSRF, Credential Theft, and Container
Escapes - David "davidrxchester" Rochester,Nicholas "gouldnicholas" Gould
DEF CON Talks - (10:30-11:30 PDT) - Root From Kilometers Away: Ubiquiti AirMax RCE - Federico Kirschbaum,Gaston
Aznarez

DEF CON Talks - Identity Crisis: Novel Vulnerabilities leading to Kerberos Downgrade, DoS, and Full Domain Takeover - Shai Laron

DEF CON Training - cont...(08:30-17:30 PDT) - Blue vs Red Bootcamp: From Attacker Playbooks to Defender Detections - Carlo Anez Mazurco, Mariana Ruiz

DEF CON Training - cont...(08:30-17:30 PDT) - Influence Operations: Tactics, Defense, and Exploitation - Greg Conti, Tom Cross

DEF CON Training - cont...(08:30-17:30 PDT) - Full-Stack Pentesting Laboratory: 100% Hands-On + Lifetime LAB Access - Dawid Czagan

DEF CON Workshops - cont...(09:00-12:59 PDT) - Sold Out - Wi-Fight Club: I am Jack's Evil Twin - James Hawk, Jon "C4V3M4N" Milkins, Brian Burnett

DEF CON Workshops - cont...(09:00-12:59 PDT) - Sold Out - Explore the Windows instrumentation callback - Yoann "OtterHacker" DEQUEKER

DEF CON Workshops - cont...(09:00-12:59 PDT) - Sold Out - Step-by-Step Malware Development: Evading EDR from Loaders to the Kernel - Yu Terada, Kotaro "@Decamark / @BinaryPoodle" Osugi

DEF CON Workshops - cont...(09:00-12:59 PDT) - Sold Out - Words As Weapons: Breaking AI and Agents; Then Securing Them - Pavan "pavanreddysec" Reddy

DEF CON Workshops - cont...(09:00-12:59 PDT) - Sold Out - HackTheCloud26: Chaining Cloud Misconfigurations to Compromise Infrastructure - HackeMate

DEF CON Workshops - cont...(09:00-12:59 PDT) - Sold Out - Hecate: A Trivial UART Tool - mx, Joe "SecurelyFitz" FitzPatrick, nyx

DEF CON Workshops - cont...(09:00-12:59 PDT) - Sold Out - Detecting and Analyzing Memory Only Malware with Volatility 3 - Andrew Case, Pierre "Abyss Watcher" Breton, David McDonald

DEF CON Workshops - cont...(09:00-12:59 PDT) - Sold Out - Battle-Tested Broadcasts: RF Insights From Ukraine - Preston Zen

Demo Labs - SecretSifter: Production Apps Are Leaking Credentials. The Blindspot DAST Never Checked. - Hemanth Gorijala

Demo Labs - Peekaboo: Breaking the Black Box of Threat and Malware Emulation - Zhassulan "cocomelonc" Zhussupov

Demo Labs - Goose Processing Unit (GPU): VRAM as an Unmonitored Attack Surface - Gannon "Dorf" Gebauer, Anthony "Coin" Rose, Hana Christensen

Demo Labs - DFMI: Weaponizing MSI Installers for Fileless Code Execution - Anil Celik

Demo Labs - Reversing F5: Pure-Go Steganography, Live Forensic Cover Recovery, and JPEG Fragility Analysis - Overkilll

Demo Labs - Monitor, Compile, Enforce: A Compiler Pipeline for Container Security Policy in Rust and eBPF - Buğrahan Yücel

Embedded Systems Village - Embedded Systems Village CTF -

Embedded Systems Village - Thread Carefully -

Embedded Systems Village - Embedded - 101 Labs -

Embedded Systems Village - Exploit Bluetooth Low Energy with BLESPlloit and optional ESP32 - Slawomir Jasek

Game Hacking Village - Riot Games Vanguard: Pwn to own -

Game Hacking Village - Chill Zone: Casual Games & TASBot Smash Demo -

Game Hacking Village - RIP Denuvo: DRM in a Post-Hypervisor World - Amin Hussien

Game Hacking Village - (10:45-11:30 PDT) - Dreamcast Ex Inferis: RCE on the Sega Dreamcast PlanetWeb Browser - Christopher Hernandez

IoT Village - All About UART -

IoT Village - Smart Home in the Matter: Blink, Race, Attack CTF -

IoT Village - Discover GE Appliances! -

IoT Village - Expose Hidden Surveillance in Everyday Tech -

IoT Village - Cat-apstrophic Hacking: Breaking Into Smart Litter Boxes -

IoT Village - Just Hacking Training -

IoT Village - Raiders of the Lost Firmware: A Hands-On Workshop in IoT Firmware Archaeology -

IoT Village - Hands-On Hardware Hacking – From JTAG to Root, Memory Patching Boot Process for Root Access -

IoT Village - (10:30-11:45 PDT) - Playing with Hyper-local Pocket-Sized Servers - Brandon

La Villa Community - Learning Deception by Doing: Attacking and Defending - Diego Staino, Fede Pacheco

La Villa Community - (10:30-10:59 PDT) - Self Hosting Nightmare - Exploiting AI models for supply chain attacks - Davidson Mizael

La Villa Community - (10:30-12:59 PDT) - Workshop Before the SIEM Blinks: How AI Memory Turns Alerts into

Intelligence - Luis Pazmino,Yoshihito Adachi
 Lockpick Village - (10:15-10:45 PDT) - Intro to Lockpicking -
 Lonely Hackers Club - Lonely Hackers Club - Sticker Swap Table -
 Lonely Hackers Club - Lonely Hackers Club - Lockpicking Table -
 Lonely Hackers Club - Lonely Hackers Club CTF -
 Lonely Hackers Club - (10:30-16:30 PDT) - Resume Review with the Lonely Hackers Club -
 Maker's Village - Makers' Village - Hacker Arts and Crafts -
 Malware Village - Cracking ValleyRAT: From Builder Secrets to Kernel Rootkits - Jiří Vinopal
 Malware Village - (10:45-11:25 PDT) - Demystifying the Playboy RaaS - Gijs Rijnders
 Malware Village - Hostile Input: PDF Triage That Survives an Adversarial Document - Klaus Wunder
 Middle Easterns & Africans in Cyber Security (MEACS) - From al-Kindi to DEF CON: The Middle Eastern and African
 Roots of Cybersecurity - Amber Bennoui,Ezz Tahoun
 Misc - Coloring Reset -
 Mobile Hacking Community - A Droidwork Orange: A Longitudinal Study of Android Security Research - Nicholas
 Miazzo,Eleonora Losiouk
 Mobile Hacking Community - Mobile Hacking Community - Open -
 Mobile Hacking Community - RedMatter: Let AI Write Your Cross-Platform Mobile Exploits - Subho Halder
 Mobile Hacking Community - Mobile Hacking - Informal CTF -
 Nix Vegas Community - Nix Vegas Opening Ceremony -
 Nix Vegas Community - (10:30-10:45 PDT) - How to piss off your Nix friends - Farid Zakaria
 Nix Vegas Community - (10:45-10:59 PDT) - Beholden to No One: The Nix Override Ladder - Daniel Baker
 Noob Community - Wanna Hack Space ? Why? Is it out of this world? - Henry Danielson Hankashyyk
 Noob Community - Break Things, Learn Things: Hands-On Hacking for Beginners - Evolve Security Academy
 Noob Community - Arcanum Security Labs -
 Noob Community - Hack The Box DC Junior Ranger Program Challenge -
 Noob Community - Mentoring and Career Advice -
 Noob Community - Kryptsec Labs -
 Noob Community - TCM Security Labs -
 Noob Community - SANS Institute NetWars Labs -
 Noob Community - Skillbit Labs -
 Noob Community - No Stupid Questions -
 Noob Community - (10:30-10:45 PDT) - The importance of Networking in Cybersecurity community - Michael Lenz
 OSINT For Good Community - OSINT4Good Community - DC NextGen Content -
 OSINT For Good Community - FINDX OSINT Educational Series -
 OSINT For Good Community - Trace Labs L150: Case Walkthrough - Brent Louie
 OWASP Foundation - BadVR: Signals Everywhere a collaboration with XR Village - Jad Meouchy,Suzanne Borders
 OWASP Foundation - Let's Play! OWASP Cornucopia for Mobile Application Security Threat Modeling - Sven Schleier
 OWASP Foundation - (10:30-10:59 PDT) - Spotlight: Choose Your Own Adventure with InfoSecMap - W. Martín Villalba
 Payment Village - (10:30-10:45 PDT) - Payment Village Intro - What's Happening at the Village -
 Policy @ DEF CON - Whose Agent Is It Anyway? Agency, Authorization, and Accountability in the Year of the AI Agent -
 Andreas Kaltsounis,Jacob Wall
 Policy @ DEF CON - Journey to Create an All-state Cybersecurity Plan for Oklahoma - Craig "jafo" Buchanan
 Radio Frequency Village - Radio Frequency Village Events -
 Radio Frequency Village - (10:30-12:25 PDT) - RF CTF Kick Off Day 2 - RF Hackers
 Recon Village - Hunting the Contagious Trader Delivery Network - Alessandra Rizzo,Ariel Ropek
 Red Team Village - From Path Traversal to Domain Credentials in 90 Seconds - Mike Lisi
 Red Team Village - PMTC: One-Click RCE and Persistent Exfil in AI Coding Agents - Ahmet Furkan Aydogan
 Red Team Village - MCP Servers: The Next Enterprise Attack Surface - Apoorwa Joshi,Justin Dray
 Red Team Village - Hands-On Autonomous Pentesting with Pentest Copilot - Dhruva Goyal,Sitaraman Subramanian
 Red Team Village - Inside the Red Team Cabal: A Decade of Lessons from Enterprise Red Teams - Jason Strange,Wes
 Thurner
 Red Team Village - Living Off the Vault - Alexandru Uifalv,Jennifer Slaybaugh,Morton Schenk
 Red Team Village - Pyramid of Pain-Red Team (Human and Technical Friction) - Frank Victory
 Scambait Village - Open Q&A -
 Scambait Village - KSCM Scambait Radio -

Social Engineering Community Village - Social Engineering Community Village - Open Hours -
Social Engineering Community Village - (10:15-13:15 PDT) - Battle of the Bots: Vishing Edition -
Social Engineering Community Village - Social Engineering 101: The Four Psychological Backdoors to Scam Your Way into
Anything - Brian Brushwood
Social Gatherings/Events - cont...(09:00-18:59 PDT) - Human Registration Open -
Social Gatherings/Events - cont...(09:00-15:59 PDT) - Merch (formerly swag) Area Open -- README -
Social Gatherings/Events - Music - SomaFM -
Telecom Village - A 5G Digital Twin CTF for Hacking Carrier-Grade Infrastructure - T-Mobile CTF Team
The Diana Initiative - MEACS: Middle Easterns & African in Cyber Security Tour -
The Diana Initiative - (10:20-10:30 PDT) - Crypto And Privacy Village Tour -
The Diana Initiative - (10:30-10:40 PDT) - Data Duplication Village Tour -
The Diana Initiative - (10:40-10:50 PDT) - Payment Village Tour -
The Diana Initiative - (10:50-10:59 PDT) - Policy @ Defcon Tour -
The Diana Initiative - Quiet Room -
The Diana Initiative - Quiet Room -
The Diana Initiative - Yoga - Deanna Heon
Voting Village - Voting Village Lab -
Voting Village - "Trust Us, It's Secure": Why Internet Voting Isn't - Barbara Simons
Voting Village - (10:30-10:59 PDT) - Software Quality in Electronic Voting - Duncan Buell

[Return to Index](#) - [Locations Legend](#)

[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Mission: Compromised - Hacking a Satellite from the Ground Up](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Drone Hacking Workshop](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Drone Hacking Choose your Own Adventure](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Flight Simulator/EFB](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [MOUSE Runner & Flappy Drone](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [SpaceCOP - Catch Me If You Can](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Nebula Showdown: Space Systems Security CTF Adventure](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Satellites Under Attack: Hands-On Satellite Security Threat Scenarios](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [SR-71 Blackbird Badge Challenge](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [DCNextGen - Bricks in the Air](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Bricks in the Air](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [DCNextGen - Space Grand Challenge - SatHack: The MOUSE-1 Mission](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [DCNextGen - RIC-1: ELT Localization Exercise - N3VR-G0N Down](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Aerospace Ecosystem Resilience Innovation Environment \(AERIE\) Cyber Range](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [ARINC 664 CTF Challenge](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Aviation ISAC Cybersecurity Challenge](#) -
[Aerospace Village](#) - [Security Analysis of Open-Source Software Used in Onboard Satellite Systems](#) - Roe Idan
[Aerospace Village](#) - (11:30-11:59 PDT) - [So You Want to Work in Aircraft Cyber? Here's what you need to know!](#) - Matt Gaffney, Marcie Wise
[AI Village](#) - cont...(10:00-17:59 PDT) - [Cyber Mirage: Realtime Deepfake Demos](#) - Brandon Kovacs
[AI Village](#) - cont...(10:00-17:59 PDT) - [Poster Presentations](#) -
[AI Village](#) - cont...(10:00-17:59 PDT) - [AI Village: Village Open](#) -
[AI Village](#) - [What is AI? Interactive, Unplugged Activity](#) - Sam Mosley
[AppSec Village](#) - cont...(10:15-11:15 PDT) - [In Untrust We Can Trust: Enforcing Trust Boundaries for Humans and AI Alike](#) - Yariv Tal
[AppSec Village](#) - (11:30-12:30 PDT) - [Precogly: Open-Source Threat Modeling for the AI-Coding Era](#) - Vikramaditya Narayan
[AppSec Village](#) - cont...(10:15-12:59 PDT) - [Prompt Injection: Attacking and Defending AI-Powered Applications](#) - Mohammed Ilyas Ahmed
[AppSec Village](#) - [What Your Coding Agent Did Last Night: Runtime Security for AI Coding Agents](#) - Inga Cherny
[AppSec Village](#) - (11:50-12:20 PDT) - [Past the Bouncer: The Limits of CSP, Eleven Years In](#) - Pedro Fortuna
[AppSec Village](#) - [Code Invaders: Stop The Insecure Code](#) - Mackenzie
[AppSec Village](#) - [Pentester vs AI: Race The Machine, In Real Life](#) - Gwendal Mognier, Samantha Pearlstein
[AppSec Village](#) - [Cards Against Vulnerabilities](#) - Patrick Smyth
[AppSec Village](#) - [SBOM Find the Flaws](#) - Dmitry Raidman
[Biohacking Village](#) - cont...(10:00-17:59 PDT) - [Embedded & Shredded: Advanced Embedded System Hacking](#) -
[Biohacking Village](#) - cont...(10:00-17:59 PDT) - [Biohacking Device Lab](#) -
[Blacks In Cyber Village](#) - [Cyber Gamechangers: Women Who Lead, Secure, and Inspire](#) - Nikkia Henderson, Arielle Baine, Jess Hoffman
[Blue Team Village](#) - [Threat Hunting 101: Beyond the Alerts](#) - Kainu ~
[Bug Bounty Village](#) - cont...(10:45-11:30 PDT) - [You're Invited to Get Hacked: Real-World Exploits in Modern Invitation Systems](#) - Ali "logic-breaker" Kabeel
[Bug Bounty Village](#) - (11:30-12:30 PDT) - [De-Sloppify: Your AI Needs a Proxy](#) - Emile "TheSyttin" Fugulin, Vitor "busf4ctor" Falcao Habibe Costa
[Call Center Village](#) - cont...(10:00-17:59 PDT) - [Call Center Village - Open](#) -
[Car Hacking Village](#) - cont...(10:00-17:59 PDT) - [Car Hacking Village Open](#) -
[Car Hacking Village](#) - cont...(10:00-16:59 PDT) - [Bomb Bot Challenge](#) -
[Cloud Village](#) - [Patch Me If You Can: Hands-On Network Threat Defense](#) - Don Bogert
[Cloud Village](#) - [From Findings to Remediations: Open Source Cloud Security at AI Speed with Prowler](#) - Toni de la Fuente, Amit Sharma

Cloud Village - cont...(10:40-11:20 PDT) - Ghost Records: Automating Dangling DNS & Subdomain Takeover Detection at Enterprise Scale - Jai Kumar Sharma,Tom McCarthy

Cloud Village - (11:20-11:59 PDT) - Trust the Cloud Pipeline, Lose the Kingdom - Shane Young

CodeBloom - Work Session: Ciphers -

Contests - cont...(10:00-11:59 PDT) - Hack3r Runw@y v8.0 -

Contests - cont...(10:00-17:59 PDT) - 5N4CK3Y -

Contests - cont...(10:00-17:59 PDT) - DC's Next Top Threat Model -

Contests - cont...(10:00-17:59 PDT) - Untechnical -

Contests - cont...(10:00-17:59 PDT) - DEF CON Scavenger Hunt -

Contests - cont...(10:00-17:59 PDT) - Darknet-NG -

Contests - cont...(10:00-17:59 PDT) - Crack Me If You Can 2026 -

Contests - cont...(10:00-17:59 PDT) - TeleChallenge -

Contests - cont...(10:00-17:59 PDT) - HackFortress -

Contests - cont...(10:00-17:59 PDT) - ?Cube -

Contests - cont...(10:00-17:59 PDT) - \$unL1ght Sh4d0w5 -

Contests - cont...(10:00-17:59 PDT) - Octopus Game - Booth Open -

Contests - cont...(10:00-17:59 PDT) - Beer Chilling Contraption Contest -

Contests - cont...(10:00-17:59 PDT) - Cryptid Hunt -

Contests - cont...(10:00-17:59 PDT) - HSPACE: AI Battlegrounds -

Contests - cont...(10:00-17:59 PDT) - spyVspy 3: Rat Race -

Contests - cont...(10:00-17:59 PDT) - Hacker Games -

Contests - cont...(10:00-17:59 PDT) - PhreakMe -

Contests - cont...(10:00-17:59 PDT) - Game Hacking Village CTF -

Contests - cont...(10:00-17:59 PDT) - Kubernetes CTF -

Contests - cont...(10:00-17:59 PDT) - Hac-Man -

Contests - cont...(10:00-17:59 PDT) - Crack the Core -

Contests - cont...(10:00-17:59 PDT) - Cyber Deck Competition -

Contests - cont...(10:00-17:59 PDT) - Pinball High Score Contest -

Contests - cont...(10:00-17:59 PDT) - Code Cadaver: Break Every System. Save Your Friend. -

Contests - cont...(10:00-17:59 PDT) - PWN UR H0M3 - DDos CTF -

Contests - cont...(10:00-17:59 PDT) - Reali7y Overrun - Contest running -

Contests - cont...(10:00-17:59 PDT) - Tin Foil Hat Contest -

Contests - cont...(10:00-17:59 PDT) - CMD+CTRL Cyber Range: DarkMoney -

Contests - cont...(10:00-17:59 PDT) - Radio Frequency Capture the Flag -

Contests - cont...(10:00-17:59 PDT) - DEF CON CTF: Benevolent Bureau of Birds -

Contests - cont...(10:00-17:59 PDT) - AI Village Plays Pokemon: DEFCON Edition - Nick Ashworth

Contests - cont...(10:00-17:59 PDT) - AI Village - Hal CTF -

Contests - cont...(10:00-11:59 PDT) - StarPWN CTF -

Contests - cont...(10:00-16:59 PDT) - Car Hacking Village CTF -

Contests - cont...(10:00-17:59 PDT) - OWASP CTF -

Contests - cont...(10:00-11:59 PDT) - Blue Team Village CTF - Project Obsidian -

Contests - cont...(10:00-17:59 PDT) - Escalation Desk CTF -

Contests - cont...(10:00-17:59 PDT) - DEF CON Groups Sticker Contest -

Contests - cont...(10:00-17:59 PDT) - DEF CON Groups Backdoors & Breaches - Tim Doerges,Seth Benning

Contests - cont...(10:00-23:59 PDT) - Apex Park (Cloud Village CTF) -

Contests - cont...(10:00-17:59 PDT) - Hacking GRC Contest -

Crypto & Privacy Village - Gold Bug: Puzzle Panel with Friends - CPV Gold Bug Team 2026,TBD

Data Duplication Village - cont...(10:00-17:59 PDT) - DDV open and accepting drives for duplication -

Data Duplication Village - Poison the Well: RAG Attacks Against the Hacking Community's Own Archives - Omer Farooq

DCNextGen - Meshpocalypse: Building Your Own Off-Grid Hacker Network - Adventures of Illya

DEF CON Groups - Building a Hacker Haven: The Long Game of Growing a Local Hacker Community - Ryan Zagrodnik,Allie Zagrodnik

DEF CON Groups - cont...(10:00-17:59 PDT) - DEF CON Groups (DCG) -

DEF CON Talks - cont...(10:00-11:59 PDT) - Car Hacking Village Scavenger Hunt Contest -

DEF CON Talks - Tracking the Trackers: How We Took Over 36 Million GPS Devices Protecting Children and Vehicles -

Felipe Solferini,Vangelis Stykas

DEF CON Talks - cont...(10:30-11:30 PDT) - [Harvest Now, Decrypt Later: Practical Attacks on Post-Quantum Cryptography Implementations](#) - Aleksandr Krasnov

DEF CON Talks - (11:30-12:30 PDT) - [Thin Client? Thin Crypto - Bypassing Full-Disk Encryption Across Three Major Thin Clients Vendors without Breaking a Cipher](#) - Darren McDonald

DEF CON Talks - [Very Pwned: Hacking Verifone's card machine three times in a row](#) - Reino Mostert

DEF CON Talks - cont...(10:30-11:30 PDT) - [Root From Kilometers Away: Ubiquiti AirMax RCE](#) - Federico Kirschbaum,Gaston Aznarez

DEF CON Talks - (11:30-12:30 PDT) - [Your OTP Never Arrived: Attacking the Trust Boundary Where SMS Meets the Internet](#) - Kyprianos "kavasilo" Vasilopoulos,Nikos "nickvourd" Vourdas

DEF CON Talks - [Forgotten but Not Gone: Unauthenticated RCEs and LPEs in Legacy Linux Services](#) - Ron Ben Yizhak

DEF CON Training - cont...(08:30-17:30 PDT) - [Blue vs Red Bootcamp: From Attacker Playbooks to Defender Detections](#) - Carlo Anez Mazurco,Mariana Ruiz

DEF CON Training - cont...(08:30-17:30 PDT) - [Influence Operations: Tactics, Defense, and Exploitation](#) - Greg Conti,Tom Cross

DEF CON Training - cont...(08:30-17:30 PDT) - [Full-Stack Pentesting Laboratory: 100% Hands-On + Lifetime LAB Access](#) - Dawid Czagan

DEF CON Workshops - cont...(09:00-12:59 PDT) - [Sold Out - Wi-Fight Club: I am Jack's Evil Twin](#) - James Hawk,Jon "C4V3M4N" Milkins,Brian Burnett

DEF CON Workshops - cont...(09:00-12:59 PDT) - [Sold Out - Explore the Windows instrumentation callback](#) - Yoann "OtterHacker" DEQUEKER

DEF CON Workshops - cont...(09:00-12:59 PDT) - [Sold Out - Step-by-Step Malware Development: Evading EDR from Loaders to the Kernel](#) - Yu Terada,Kotaro "@Decamark / @BinaryPoodle" Osugi

DEF CON Workshops - cont...(09:00-12:59 PDT) - [Sold Out - Words As Weapons: Breaking AI and Agents; Then Securing Them](#) - Pavan "pavanreddysec" Reddy

DEF CON Workshops - cont...(09:00-12:59 PDT) - [Sold Out - HackTheCloud26: Chaining Cloud Misconfigurations to Compromise Infrastructure](#) - HackeMate

DEF CON Workshops - cont...(09:00-12:59 PDT) - [Sold Out - Hecate: A Trivial UART Tool](#) - mx,Joe "SecurelyFitz" FitzPatrick,nyx

DEF CON Workshops - cont...(09:00-12:59 PDT) - [Sold Out - Detecting and Analyzing Memory Only Malware with Volatility 3](#) - Andrew Case,Pierre "Abyss Watcher" Breton,David McDonald

DEF CON Workshops - cont...(09:00-12:59 PDT) - [Sold Out - Battle-Tested Broadcasts: RF Insights From Ukraine](#) - Preston Zen

Demo Labs - [GhostCatcher \(endpoint detection agent\)](#) - Sercan Okur

Demo Labs - [sisakulint:CI-Friendly static linter with autofix, SAST, semantic analysis for GitHub Actions](#) - Atsushi Sada,hikae

Demo Labs - [Clew: Untangling Evasive Malware with Per-Sample Fuzzing Seeds](#) - Kyler McElroy,Anita Ding,Daniel Koranek

Demo Labs - [X-Ray Your Agents: Pentesting MCPs, Skills, and the Plugin Supply Chain](#) - Xia Hua,Abhijeet Kumar

Demo Labs - [TokenMesh: Exposing Azure's Hidden Identity Attack Surface](#) - Saksham Agrawal

Demo Labs - [pymssi: Interactive MSI Installer Analysis in Python and the Browser](#) - Ryan "Nightlark" Mast

Embedded Systems Village - cont...(10:00-17:59 PDT) - [Embedded Systems Village CTF](#) -

Embedded Systems Village - cont...(10:00-17:59 PDT) - [Thread Carefully](#) -

Embedded Systems Village - cont...(10:00-17:59 PDT) - [Embedded - 101 Labs](#) -

Embedded Systems Village - cont...(10:00-17:59 PDT) - [Exploit Bluetooth Low Energy with BLESPlloit and optional ESP32](#) - Slawomir Jasek

Game Hacking Village - cont...(10:00-16:59 PDT) - [Riot Games Vanguard: Pwn to own](#) -

Game Hacking Village - cont...(10:00-15:59 PDT) - [Chill Zone: Casual Games & TASBot Smash Demo](#) -

Game Hacking Village - cont...(10:45-11:30 PDT) - [Dreamcast Ex Inferis: RCE on the Sega Dreamcast PlanetWeb Browser](#) - Christopher Hernandez

Game Hacking Village - (11:30-11:59 PDT) - [Catching Cheaters in Super Smash Bros Melee](#) - AltF4

Hackers.town - [How to get RCE on a car](#) - Ac0rn

Ham Radio Village - [Digital Modes 101: The Weird, Wonderful World of Computer Radio](#) - Jon Marler (K4CHN)

ICS Village - (11:30-11:59 PDT) - [Nuclear Industrial Control System Simulation \(NICSSIM\) aka Multi-Agent Cyber Defense Framework for Distributed Nuclear Operational Technology Systems](#) - Carmela Gonzales,Brian G. Rodiles Delgado,Marco A.

Alanis Komiyama

IoT Village - cont...(10:00-17:59 PDT) - [Smart Home in the Matter: Blink, Race, Attack CTF](#) -

IoT Village - cont...(10:00-17:59 PDT) - [Expose Hidden Surveillance in Everyday Tech](#) -

IoT Village - cont...(10:00-17:59 PDT) - [Discover GE Appliances!](#) -

IoT Village - cont...(10:00-17:59 PDT) - [All About UART](#) -

IoT Village - cont...(10:00-17:59 PDT) - [Raiders of the Lost Firmware: A Hands-On Workshop in IoT Firmware Archaeology](#) -

-

IoT Village - cont...(10:00-17:59 PDT) - [Just Hacking Training](#) -

IoT Village - cont...(10:00-17:59 PDT) - [Cat-astrophic Hacking: Breaking Into Smart Litter Boxes](#) -

IoT Village - cont...(10:00-17:59 PDT) - [Hands-On Hardware Hacking – From JTAG to Root, Memory Patching Boot Process for Root Access](#) -

IoT Village - cont...(10:30-11:45 PDT) - [Playing with Hyper-local Pocket-Sized Servers](#) - Brandon

IoT Village - [The Camera Is Lying: RTSP Trust Failures in Modern Surveillance Systems](#) - Bogdan "BOTEZATU"

IoT Village - (11:45-12:30 PDT) - [Anyone Can Hack IoT \(Even Easier Now\) - A Beginner's Guide to AI Augmented IoT Hacking](#) - Andrew Bellini

La Villa Community - [Meet XEntry Team: A powerful threat actor abusing Bitlocker for ransomware](#) - Eduardo Chavarro Ovalle

La Villa Community - cont...(10:30-12:59 PDT) - [Workshop Before the SIEM Blinks: How AI Memory Turns Alerts into Intelligence](#) - Luis Pazmino, Yoshihito Adachi

Lockpick Village - [Classic US High Sec: how to pick a Medeco](#) - Max A

Lonely Hackers Club - cont...(10:00-17:59 PDT) - [Lonely Hackers Club - Sticker Swap Table](#) -

Lonely Hackers Club - cont...(10:00-17:59 PDT) - [Lonely Hackers Club - Lockpicking Table](#) -

Lonely Hackers Club - cont...(10:00-17:59 PDT) - [Lonely Hackers Club CTF](#) -

Lonely Hackers Club - cont...(10:30-16:30 PDT) - [Resume Review with the Lonely Hackers Club](#) -

Maker's Village - cont...(10:00-17:59 PDT) - [Makers' Village - Hacker Arts and Crafts](#) -

Maker's Village - [Build-A-Badge Workshop](#) - hunny, Teazee, Buddha, MLP, M-Nelly, Alchemmer

Malware Village - cont...(10:45-11:25 PDT) - [Demystifying the Playboy RaaS](#) - Gijs Rijnders

Malware Village - (11:35-12:15 PDT) - [Haetae: An Agent to Takedown North Korean C2 Servers](#) - Nelson Colon

Malware Village - cont...(10:10-12:10 PDT) - [Hostile Input: PDF Triage That Survives an Adversarial Document](#) - Klaus Wunder

Mobile Hacking Community - cont...(10:00-17:59 PDT) - [Mobile Hacking - Informal CTF](#) -

Mobile Hacking Community - cont...(10:00-17:59 PDT) - [Mobile Hacking Community - Open](#) -

Mobile Hacking Community - (11:15-12:15 PDT) - [An Android voyage from Java to Smali with ASM](#) - Ricardo Loura

Nix Vegas Community - (11:30-11:59 PDT) - [Compiling the World: A Binary Dataset Built from nixpkgs](#) - Chris Connelly

Noob Community - cont...(10:00-17:59 PDT) - [No Stupid Questions](#) -

Noob Community - cont...(10:00-17:59 PDT) - [SANS Institute NetWars Labs](#) -

Noob Community - cont...(10:00-17:59 PDT) - [Skillbit Labs](#) -

Noob Community - cont...(10:00-17:59 PDT) - [TCM Security Labs](#) -

Noob Community - cont...(10:00-17:59 PDT) - [Arcanum Security Labs](#) -

Noob Community - cont...(10:00-17:59 PDT) - [Mentoring and Career Advice](#) -

Noob Community - cont...(10:00-17:59 PDT) - [Hack The Box DC Junior Ranger Program Challenge](#) -

Noob Community - cont...(10:00-17:59 PDT) - [Kryptsec Labs](#) -

Noob Community - cont...(10:00-11:20 PDT) - [Break Things, Learn Things: Hands-On Hacking for Beginners](#) - Evolve Security Academy

Noob Community - [No One Makes It Alone - Community as the Ultimate Security Control](#) - Kristen Sanders

Noob Community - (11:30-12:50 PDT) - [OASIS: Prompt to Pwn](#) - Marshall Livingston

Noob Community - (11:45-12:45 PDT) - [Gamifying the Matrix: a MITRE ATT&CK Video Game](#) - Annie Meaney, Anne Drago

OSINT For Good Community - cont...(10:00-17:59 PDT) - [OSINT4Good Community - DC NextGen Content](#) -

OSINT For Good Community - cont...(10:00-17:59 PDT) - [FINDX OSINT Educational Series](#) -

OSINT For Good Community - (11:15-11:45 PDT) - [CTF Intro, Quick Guides, and Rule Review](#) - Kenny J

OWASP Foundation - cont...(10:00-17:59 PDT) - [BadVR: Signals Everywhere a collaboration with XR Village](#) - Jad Meouchy, Suzanne Borders

OWASP Foundation - [Oh hai! Meet Tanya "SheHacksPurple" Janca](#) - Tanya "SheHacksPurple" Janca

Payment Village - [Victim as a Service: Engaging with Trust-Based Scams Using AI](#) - Ariana Mirian

[Payment Village - \(11:30-11:50 PDT\) - Introduction to Vulnerable ATM Badge - Vincent Sloan](#)
[Physical Security Village - No Entry: Badge Access Denial on Demand - Andrew Quill](#)
[Policy @ DEF CON - From Policy to Prod: How a Frontier AI Lab Enforces its Cyber Rules - Grant Versfeld,David "0xdf" Forsythe](#)
[Queercon Community - Polycon -](#)
[Radio Frequency Village - cont...\(10:00-17:59 PDT\) - Radio Frequency Village Events -](#)
[Radio Frequency Village - cont...\(10:30-12:25 PDT\) - RF CTF Kick Off Day 2 - RF Hackers](#)
[Recon Village - cont...\(10:00-12:30 PDT\) - Hunting the Contagious Trader Delivery Network - Alessandra Rizzo,Ariel Ropek](#)
[Recon Village - GE\(O\)SINT Contest -](#)
[Red Team Village - cont...\(10:00-11:59 PDT\) - From Path Traversal to Domain Credentials in 90 Seconds - Mike Lisi](#)
[Red Team Village - cont...\(10:00-11:59 PDT\) - PMTC: One-Click RCE and Persistent Exfil in AI Coding Agents - Ahmet Furkan Aydogan](#)
[Red Team Village - cont...\(10:00-11:59 PDT\) - MCP Servers: The Next Enterprise Attack Surface - Apoorwa Joshi,Justin Dray](#)
[Red Team Village - cont...\(10:00-11:59 PDT\) - Hands-On Autonomous Pentesting with Pentest Copilot - Dhruva Goyal,Sitaraman Subramanian](#)
[Red Team Village - DPAPI Is Not a Boundary: A Full Infostealer Kill Chain Operators Can Replicate - Filipi Pires](#)
[Red Team Village - The Authentic Operator: Social Engineering Through Natural Delivery - Joanna -](#)
[Red Team Village - cont...\(10:00-11:59 PDT\) - Living Off the Vault - Alexandru Uifalv,Jennifer Slaybaugh,Morton Schenk](#)
[Red Team Village - cont...\(10:00-11:59 PDT\) - Pyramid of Pain-Red Team \(Human and Technical Friction\) - Frank Victory](#)
[Scambait Village - cont...\(10:00-17:59 PDT\) - Open Q&A -](#)
[Scambait Village - cont...\(10:00-17:59 PDT\) - KSCM Scambait Radio -](#)
[Social Engineering Community Village - cont...\(10:00-17:59 PDT\) - Social Engineering Community Village - Open Hours -](#)
[Social Engineering Community Village - cont...\(10:15-13:15 PDT\) - Battle of the Bots: Vishing Edition -](#)
[Social Engineering Community Village - \(11:30-12:30 PDT\) - Social Engineering 101: The Four Psychological Backdoors to Scam Your Way into Anything - Brian Brushwood](#)
[Social Gatherings/Events - cont...\(09:00-18:59 PDT\) - Human Registration Open -](#)
[Social Gatherings/Events - Book Signing - Aamiruddin Syed - Aamiruddin Syed](#)
[Social Gatherings/Events - Book Signing - Cindy Cohn - Cindy Cohn](#)
[Social Gatherings/Events - cont...\(09:00-15:59 PDT\) - Merch \(formerly swag\) Area Open -- README -](#)
[Social Gatherings/Events - cont...\(10:00-18:59 PDT\) - Music - SomaFM -](#)
[Social Gatherings/Events - Free Ham Radio License Exams -](#)
[Telecom Village - Threats in Space: The Dangerous Rise of GNSS Attacks - Isabel Manjarrez](#)
[Telecom Village - \(11:45-12:30 PDT\) - From ONT to STB: Detecting IPTV Attack Chains in the Telecom SOC - Zibran Sayyed](#)
[The Diana Initiative - Biohacking Village Tour -](#)
[The Diana Initiative - Adversary Village Tour -](#)
[The Diana Initiative - \(11:20-11:30 PDT\) - Radio Frequency Village Tour -](#)
[The Diana Initiative - \(11:30-11:40 PDT\) - Embedded System Village Tour -](#)
[The Diana Initiative - \(11:40-11:50 PDT\) - Gamer Village Tour -](#)
[The Diana Initiative - \(11:50-11:59 PDT\) - Queercon Community Lounge Tour -](#)
[The Diana Initiative - Stay Sharp: Navigating Pen Testing and Bug Bounty in an AI-Driven World - Dana Pirvu](#)
[Voting Village - cont...\(10:00-17:59 PDT\) - Voting Village Lab -](#)
[Voting Village - Liberty and Justice for All - Michael Moore](#)
[Voting Village - \(11:30-11:59 PDT\) - Are We Making Things Worse? Election Denialism and Security Research - Matt Blaze,Geoff Hale,Michael Moore,Kendall Spencer,Philip Stark](#)

[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Nebula Showdown: Space Systems Security CTF Adventure](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Satellites Under Attack: Hands-On Satellite Security Threat Scenarios](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [SR-71 Blackbird Badge Challenge](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [SpaceCOP - Catch Me If You Can](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Flight Simulator/EFB](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Drone Hacking Workshop](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Mission: Compromised - Hacking a Satellite from the Ground Up](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Drone Hacking Choose your Own Adventure](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [MOUSE Runner & Flappy Drone](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [ARINC 664 CTF Challenge](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Aviation ISAC Cybersecurity Challenge](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Aerospace Ecosystem Resilience Innovation Environment \(AERIE\) Cyber Range](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [DCNextGen - Bricks in the Air](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Bricks in the Air](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [DCNextGen - Space Grand Challenge - SatHack: The MOUSE-1 Mission](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [DCNextGen - RIC-1: ELT Localization Exercise - N3VR-G0N Down](#) -
[AI Village](#) - cont...(10:00-17:59 PDT) - [AI Village: Village Open](#) -
[AI Village](#) - cont...(10:00-17:59 PDT) - [Cyber Mirage: Realtime Deepfake Demos](#) - Brandon Kovacs
[AI Village](#) - cont...(10:00-17:59 PDT) - [Poster Presentations](#) -
[AI Village](#) - [This Wasn't AI Generated: Principles for Breaking Generative Watermarks](#) - Thomas Mason,Tahseen Rabbani
[AI Village](#) - [AgentBreaker: A blind spot detector for your coding agents](#) - Aditi Narasimhan,Farzaan Kaiyom
[AppSec Village](#) - cont...(11:30-12:30 PDT) - [Precogly: Open-Source Threat Modeling for the AI-Coding Era](#) - Vikramaditya Narayan
[AppSec Village](#) - (12:45-13:45 PDT) - [OWASP FinBot CTF: Hands-On Agentic AI Threats](#) - Helen Oakley,saikishu
[AppSec Village](#) - cont...(10:15-12:59 PDT) - [Prompt Injection: Attacking and Defending AI-Powered Applications](#) - Mohammed Ilyas Ahmed
[AppSec Village](#) - cont...(11:50-12:20 PDT) - [Past the Bouncer: The Limits of CSP, Eleven Years In](#) - Pedro Fortuna
[AppSec Village](#) - (12:30-12:59 PDT) - [Threat Modeling LLMs with PHANTOM-B](#) - Adam Shostack
[AppSec Village](#) - cont...(11:00-12:59 PDT) - [Code Invaders: Stop The Insecure Code](#) - Mackenzie
[AppSec Village](#) - cont...(11:00-12:59 PDT) - [Pentester vs AI: Race The Machine, In Real Life](#) - Gwendal Mognier,Samantha Pearlstein
[AppSec Village](#) - cont...(11:00-12:59 PDT) - [Cards Against Vulnerabilities](#) - Patrick Smyth
[AppSec Village](#) - cont...(11:00-12:59 PDT) - [SBOM Find the Flaws](#) - Dmitry Raidman
[Biohacking Village](#) - cont...(10:00-17:59 PDT) - [Embedded & Shredded: Advanced Embedded System Hacking](#) -
[Biohacking Village](#) - cont...(10:00-17:59 PDT) - [Biohacking Device Lab](#) -
[Blacks In Cyber Village](#) - [Root Access: An APT Analysis of Systemic Gatekeeping in Cybersecurity](#) - Dr. Hassan Karim
[Blacks In Cyber Village](#) - (12:30-12:55 PDT) - [The Voice Behind the Payload: Tracing AAVE Across Malware Artifacts](#) - Brett Alexander Tolbert
[Blue Team Village](#) - [Cloud Forensics 101 : Ghost in the logs](#) - Cassandra (muteki) Young,Dimple Gajra
[Bug Bounty Village](#) - [Killing AI Slop: A Multi-Model Orchestration Framework That Only Reports Findings It Can Prove](#) - Armaan Pathan
[Bug Bounty Village](#) - (12:30-12:59 PDT) - [Eating Our Own Dogfood: Running a Bug Bounty Program on a Bug Bounty Platform](#) - Shrimant Subhash More,Martzen Haagsma
[Bug Bounty Village](#) - cont...(11:30-12:30 PDT) - [De-Sloppify: Your AI Needs a Proxy](#) - Emile "TheSyttten" Fugulin,Vitor "busf4ctor" Falcao Habibe Costa
[Bug Bounty Village](#) - (12:30-13:30 PDT) - [Better Bug Hunting on AI Products: A VRP Lead's Perspective](#) - John Kotheimer
[Call Center Village](#) - cont...(10:00-17:59 PDT) - [Call Center Village - Open](#) -
[Car Hacking Village](#) - cont...(10:00-16:59 PDT) - [Bomb Bot Challenge](#) -
[Car Hacking Village](#) - cont...(10:00-17:59 PDT) - [Car Hacking Village Open](#) -
[Cloud Village](#) - cont...(11:00-12:59 PDT) - [Patch Me If You Can: Hands-On Network Threat Defense](#) - Don Bogert

[Cloud Village](#) - cont...(11:00-12:59 PDT) - [From Findings to Remediations: Open Source Cloud Security at AI Speed with Prowler](#) - Toni de la Fuente,Amit Sharma
[Cloud Village](#) - [Whose Resource Is It Anyway? The Design Flaw That Breaks the IAM Permission Model](#) - Moshe Berntsein
[Cloud Village](#) - (12:20-12:59 PDT) - [Pinchy Gets Played: How We Red-Teamed AI Agents Before the Threats Did](#) - Doron Kapah
[CodeBloom](#) - [Game Time: Input, Output, and Variables](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [5N4CK3Y](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [DC's Next Top Threat Model](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Untechnical](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [DEF CON Scavenger Hunt](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Darknet-NG](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Crack Me If You Can 2026](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [TeleChallenge](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [HackFortress](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [?Cube](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [\\$unLight Sh4d0w5](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Octopus Game - Booth Open](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Beer Chilling Contraption Contest](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Cryptid Hunt](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [HSPACE: AI Battlegrounds](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [spyVspy 3: Rat Race](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Hacker Games](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [PhreakMe](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Game Hacking Village CTF](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Kubernetes CTF](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Hac-Man](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Crack the Core](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Cyber Deck Competition](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Pinball High Score Contest](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Code Cadaver: Break Every System. Save Your Friend.](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [PWN UR H0M3 - DDoS CTF](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Real7y Overrun - Contest running](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Tin Foil Hat Contest](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [CMD+CTRL Cyber Range: DarkMoney](#) -
[Contests](#) - [Dozier Drill Tournament](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Radio Frequency Capture the Flag](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [DEF CON CTF: Benevolent Bureau of Birds](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [AI Village - Hal CTF](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [AI Village Plays Pokemon: DEFCON Edition](#) - Nick Ashworth
[Contests](#) - cont...(10:00-16:59 PDT) - [Car Hacking Village CTF](#) -
[Contests](#) - [Global OSINT Search Party CTF – DEF CON 34 Edition](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [OWASP CTF](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Escalation Desk CTF](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [DEF CON Groups Backdoors & Breaches](#) - Tim Doerges,Seth Benning
[Contests](#) - cont...(10:00-17:59 PDT) - [DEF CON Groups Sticker Contest](#) -
[Contests](#) - cont...(10:00-23:59 PDT) - [Apex Park \(Cloud Village CTF\)](#) -
[Contests](#) - [BIC Village Capture the Flag \(CTF\)](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Hacking GRC Contest](#) -
[Data Duplication Village](#) - cont...(10:00-17:59 PDT) - [DDV open and accepting drives for duplication](#) -
[Data Duplication Village](#) - (12:15-12:45 PDT) - [Forcing Physical Interlocks into Data Transit and Storage Replication](#) - Mehmet Önder Key,Temel Demir
[DCNextGen](#) - [AI and You: Staying Safe in the AI Era](#) - Zoe Reid+Echo419
[DEF CON Groups](#) - cont...(10:00-17:59 PDT) - [DEF CON Groups \(DCG\)](#) -
[DEF CON Talks](#) - [Rage Against the Sandbox: Bypassing Apple's iOS Security to Run Unsigned Code via SSH](#) - Yuval Hanoch Hirschenbein Sadde

DEF CON Talks - cont...(11:30-12:30 PDT) - Thin Client? Thin Crypto - Bypassing Full-Disk Encryption Across Three Major Thin Clients Vendors without Breaking a Cipher - Darren McDonald

DEF CON Talks - (12:30-13:30 PDT) - Writing to Shadow Stacks - Vladimir "G1ND1L4" Tokarev

DEF CON Talks - C(2)YA: Inside the Adversary's Inbox - Vitaly Simonovich

DEF CON Talks - cont...(11:30-12:30 PDT) - Your OTP Never Arrived: Attacking the Trust Boundary Where SMS Meets the Internet - Kyprianos "kavasilo" Vasilopoulos,Nikos "nickvourd" Vourdas

DEF CON Talks - (12:30-13:30 PDT) - Compounding Interest: Exploiting the ATM Supply Chain - Matt Burch

DEF CON Talks - The Glass Perimeter: Systematic Bypasses in Biometric Frameworks and the Rise of Synthetic Identity - Dan Borgogno,Javier Bernardo

DEF CON Training - cont...(08:30-17:30 PDT) - Blue vs Red Bootcamp: From Attacker Playbooks to Defender Detections - Carlo Anez Mazurco,Mariana Ruiz

DEF CON Training - cont...(08:30-17:30 PDT) - Influence Operations: Tactics, Defense, and Exploitation - Greg Conti,Tom Cross

DEF CON Training - cont...(08:30-17:30 PDT) - Full-Stack Pentesting Laboratory: 100% Hands-On + Lifetime LAB Access - Dawid Czagan

DEF CON Workshops - cont...(09:00-12:59 PDT) - Sold Out - Wi-Fight Club: I am Jack's Evil Twin - James Hawk,Jon "C4V3M4N" Milkins,Brian Burnett

DEF CON Workshops - cont...(09:00-12:59 PDT) - Sold Out - Explore the Windows instrumentation callback - Yoann "OtterHacker" DEQUEKER

DEF CON Workshops - cont...(09:00-12:59 PDT) - Sold Out - Step-by-Step Malware Development: Evading EDR from Loaders to the Kernel - Yu Terada,Kotaro "@Decamark / @BinaryPoodle" Osugi

DEF CON Workshops - cont...(09:00-12:59 PDT) - Sold Out - Words As Weapons: Breaking AI and Agents; Then Securing Them - Pavan "pavanreddysec" Reddy

DEF CON Workshops - cont...(09:00-12:59 PDT) - Sold Out - HackTheCloud26: Chaining Cloud Misconfigurations to Compromise Infrastructure - HackeMate

DEF CON Workshops - cont...(09:00-12:59 PDT) - Sold Out - Hecate: A Trivial UART Tool - mx,Joe "SecurelyFitz" FitzPatrick,nyx

DEF CON Workshops - cont...(09:00-12:59 PDT) - Sold Out - Detecting and Analyzing Memory Only Malware with Volatility 3 - Andrew Case,Pierre "Abyss Watcher" Breton,David McDonald

DEF CON Workshops - cont...(09:00-12:59 PDT) - Sold Out - Battle-Tested Broadcasts: RF Insights From Ukraine - Preston Zen

Demo Labs - Phasmid: Deniable Storage for Rubber-Hose Scenarios - Makoto "Mr.Rabbit" Sugita

Demo Labs - MSCodePhish: Redeem Your Coupon. Surrender Your Session - Raunak "Trouble1" Parmar,Chirag "3xpl01tc0d3r" Savla

Demo Labs - Keychecker : SSH Key based attack tool for DVCS Systems - Anant Shrivastava

Demo Labs - Zealot: An Autonomous Cloud Offensive Multi-Agent System - Chen Doytshman

Demo Labs - Beyond Spidering: Behavior Driven DAST for Real Application Workflows - Sara "testingSoul" Martinez

Demo Labs - Empire 7: Shipping a C2 at AI Speed - Vincent "Vinnybod" Rose,Jake "Hubbl3" Krasnov,Anthony "Coin" Rose

Embedded Systems Village - cont...(10:00-17:59 PDT) - Exploit Bluetooth Low Energy with BLESPlloit and optional ESP32 - Slawomir Jasek

Embedded Systems Village - cont...(10:00-17:59 PDT) - Thread Carefully -

Embedded Systems Village - cont...(10:00-17:59 PDT) - Embedded - 101 Labs -

Embedded Systems Village - cont...(10:00-17:59 PDT) - Embedded Systems Village CTF -

Game Hacking Village - cont...(10:00-16:59 PDT) - Riot Games Vanguard: Pwn to own -

Game Hacking Village - cont...(10:00-15:59 PDT) - Chill Zone: Casual Games & TASBot Smash Demo -

Game Hacking Village - Game Hacking with AI - Juno

Hackers.town - KYC and XMR... FOR HACKERS! - AltKey

Hackers.town - Take Back Your Memories - Patrick Sliney

Ham Radio Village - So You Got Your License, Now What? - Danny Quist

ICS Village - Local Language Models in OT - Basics and Considerations - Vivek Ponnada

IoT Village - cont...(10:00-17:59 PDT) - Expose Hidden Surveillance in Everyday Tech -

IoT Village - cont...(10:00-17:59 PDT) - Smart Home in the Matter: Blink, Race, Attack CTF -

IoT Village - cont...(10:00-17:59 PDT) - Discover GE Appliances! -

IoT Village - cont...(10:00-17:59 PDT) - All About UART -

IoT Village - cont...(10:00-17:59 PDT) - Cat-astrophic Hacking: Breaking Into Smart Litter Boxes -

IoT Village - cont...(10:00-17:59 PDT) - Hands-On Hardware Hacking – From JTAG to Root, Memory Patching Boot Process for Root Access -

IoT Village - cont...(10:00-17:59 PDT) - Just Hacking Training -

IoT Village - cont...(10:00-17:59 PDT) - Raiders of the Lost Firmware: A Hands-On Workshop in IoT Firmware Archaeology -

IoT Village - Wi-Fi Self Defense & Hacker Hunting & For Beginners - Kody Kinzie

IoT Village - cont...(11:45-12:30 PDT) - Anyone Can Hack IoT (Even Easier Now) - A Beginner's Guide to AI Augmented IoT Hacking - Andrew Bellini

IoT Village - (12:30-13:30 PDT) - Raiders of the Lost Firmware: A Hands-On Workshop in IoT Firmware Archaeology - Simone Bossi, Luca Borzacchiello

La Villa Community - Malware Inc.: Cybercrime-as-a-Service y la economía del cibercrimen moderno - Isabel Manjarrez

La Villa Community - (12:30-13:30 PDT) - Descubrimiento Industrializado de CVEs con Agentes de IA - Simon Correa, Michael Rivera

La Villa Community - cont...(10:30-12:59 PDT) - Workshop Before the SIEM Blinks: How AI Memory Turns Alerts into Intelligence - Luis Pazmino, Yoshihito Adachi

Lonely Hackers Club - cont...(10:00-17:59 PDT) - Lonely Hackers Club - Sticker Swap Table -

Lonely Hackers Club - cont...(10:00-17:59 PDT) - Lonely Hackers Club CTF -

Lonely Hackers Club - cont...(10:00-17:59 PDT) - Lonely Hackers Club - Lockpicking Table -

Lonely Hackers Club - cont...(10:30-16:30 PDT) - Resume Review with the Lonely Hackers Club -

Maker's Village - cont...(10:00-17:59 PDT) - Makers' Village - Hacker Arts and Crafts -

Maker's Village - cont...(11:00-12:30 PDT) - Build-A-Badge Workshop - hunny, Teazee, Buddha, MLP, M-Nelly, Alchemmer

Malware Village - cont...(11:35-12:15 PDT) - Haetae: An Agent to Takedown North Korean C2 Servers - Nelson Colon

Malware Village - cont...(10:10-12:10 PDT) - Hostile Input: PDF Triage That Survives an Adversarial Document - Klaus Wunder

Malware Village - (12:55-14:05 PDT) - A hands-on hour with IDA: reverse-engineer a real DLL-sideload attack from safe, purpose-built samples. No experience required — you'll crack your first binary in the first ten minutes. - David Rushmer

Maritime Hacking Village - Please Place Your Electronic Devices in {Maritime} Mode: Exposing NTN's Maritime Attack Surface - Jason Veara

Maritime Hacking Village - (12:30-12:59 PDT) - Maritime Threat Hunting: What We Actually Find When We Look - Cliff Neve, Philip Acosta, Dean Macris

Misc - (12:30-12:59 PDT) - Donating Bone Marrow: A Donor's First-Hand Experience -

Misc - Friendship Bracelets -

Mobile Hacking Community - cont...(10:00-17:59 PDT) - Mobile Hacking - Informal CTF -

Mobile Hacking Community - cont...(10:00-17:59 PDT) - Mobile Hacking Community - Open -

Mobile Hacking Community - cont...(11:15-12:15 PDT) - An Android voyage from Java to Smali with ASM - Ricardo Loura

Mobile Hacking Community - (12:30-12:59 PDT) - Triage vs. Reality: Mobile Security Findings in Bug Bounty - fr4vian

Noob Community - cont...(10:00-17:59 PDT) - Skillbit Labs -

Noob Community - cont...(10:00-17:59 PDT) - TCM Security Labs -

Noob Community - cont...(10:00-17:59 PDT) - SANS Institute NetWars Labs -

Noob Community - cont...(10:00-17:59 PDT) - No Stupid Questions -

Noob Community - cont...(10:00-17:59 PDT) - Mentoring and Career Advice -

Noob Community - cont...(10:00-17:59 PDT) - Kryptsec Labs -

Noob Community - cont...(10:00-17:59 PDT) - Arcanum Security Labs -

Noob Community - cont...(10:00-17:59 PDT) - Hack The Box DC Junior Ranger Program Challenge -

Noob Community - cont...(11:30-12:50 PDT) - OASIS: Prompt to Pwn - Marshall Livingston

Noob Community - cont...(11:45-12:45 PDT) - Gamifying the Matrix: a MITRE ATT&CK Video Game - Annie Meaney, Anne Drago

OSINT For Good Community - cont...(10:00-17:59 PDT) - OSINT4Good Community - DC NextGen Content -

OSINT For Good Community - cont...(10:00-17:59 PDT) - FINDX OSINT Educational Series -

OWASP Foundation - cont...(10:00-17:59 PDT) - BadVR: Signals Everywhere a collaboration with XR Village - Jad Meouchy, Suzanne Borders

OWASP Foundation - Oh hai! Meet Jason Haddix - Jason "jhaddix" Haddix

Payment Village - Breaking PBKDF - Adversarial Cryptanalysis and Techniques for Hunting Cryptographic Flaws - Ken Pyle

Policy @ DEF CON - (12:30-13:30 PDT) - Privacy You Inherit: How Cultural History Writes the Source Code for AI Surveillance Policy - Tati

[Policy @ DEF CON - Europe's Expanding Role in Global Vulnerability Management](#) - Nuno Rodrigues Carvalho,Razvan Gavrilă
[Queercon Community - Trans Meetup](#) -
[Radio Frequency Village - cont...\(10:00-17:59 PDT\)](#) - [Radio Frequency Village Events](#) -
[Radio Frequency Village - cont...\(10:30-12:25 PDT\)](#) - [RF CTF Kick Off Day 2](#) - RF Hackers
[Radio Frequency Village - \(12:30-13:25 PDT\)](#) - [Neotropolis: The Making of the Railgun Trackers](#) - John O'Connor
[Recon Village - cont...\(10:00-12:30 PDT\)](#) - [Hunting the Contagious Trader Delivery Network](#) - Alessandra Rizzo,Ariel Ropek
[Recon Village - cont...\(11:00-16:59 PDT\)](#) - [GE\(O\)SINT Contest](#) -
[Recon Village - Live Recon Contest](#) -
[Recon Village - TrackTheFugitive Contest](#) -
[Recon Village - \(12:40-15:10 PDT\)](#) - [The Hard Part of ASM: Ownership Attribution](#) - Jeff Foley
[Red Team Village - Ouroboros Attack! Recursive AI-Assisted 0-Day Hunting](#) - Mehmet Önder Key,Temel Demir
[Red Team Village - Command & Conquer: Hands-on C2 Primer with Mythic](#) - Logan MacLaren
[Red Team Village - Building Hackbots](#) - Jason "jhaddix" Haddix,Ryan Bonner
[Red Team Village - Red Teaming Kubernetes: From App-Level CVEs to Full Cluster Takeover](#) - Lenin Alevski
[Red Team Village - Agentic AI Supply chain Vulnerability lab](#) - Aamiruddin Syed,N A
[Red Team Village - The Protocol-Native Adversary: Full-Spectrum ICS Simulation via SiL](#) - Blessen Thomas,Javier Hernández,Wojciech Poparda
[Scambait Village - cont...\(10:00-17:59 PDT\)](#) - [KSCM Scambait Radio](#) -
[Scambait Village - cont...\(10:00-17:59 PDT\)](#) - [Open Q&A](#) -
[Scambait Village - \(12:30-13:59 PDT\)](#) - [Scammers Don't Discriminate](#) - DolphinVG
[Social Engineering Community Village - cont...\(10:00-17:59 PDT\)](#) - [Social Engineering Community Village - Open Hours](#) -
[Social Engineering Community Village - cont...\(10:15-13:15 PDT\)](#) - [Battle of the Bots: Vishing Edition](#) -
[Social Engineering Community Village - cont...\(11:30-12:30 PDT\)](#) - [Social Engineering 101: The Four Psychological Backdoors to Scam Your Way into Anything](#) - Brian Brushwood
[Social Gatherings/Events - cont...\(09:00-18:59 PDT\)](#) - [Human Registration Open](#) -
[Social Gatherings/Events - cont...\(11:00-12:59 PDT\)](#) - [Book Signing - Aamiruddin Syed](#) - Aamiruddin Syed
[Social Gatherings/Events - Book Signing - Laura Scherling](#) - Laura Scherling
[Social Gatherings/Events - cont...\(09:00-15:59 PDT\)](#) - [Merch \(formerly swag\) Area Open -- README](#) -
[Social Gatherings/Events - cont...\(10:00-18:59 PDT\)](#) - [Music - SomaFM](#) -
[Social Gatherings/Events - Friends of Bill W](#) -
[Social Gatherings/Events - cont...\(11:00-16:59 PDT\)](#) - [Free Ham Radio License Exams](#) -
[Telecom Village - cont...\(11:45-12:30 PDT\)](#) - [From ONT to STB: Detecting IPTV Attack Chains in the Telecom SOC](#) - Zibran Sayyed
[Telecom Village - \(12:30-12:59 PDT\)](#) - [Signaling Sabotage: Why 100% Compliance is 0% Security](#) - Vinod Shrimali
[The Diana Initiative - Kubernetes CTF at DEF CON Contest Tour](#) -
[The Diana Initiative - Malware Village Tour](#) -
[The Diana Initiative - \(12:20-12:30 PDT\)](#) - [Blue Team Village Tour](#) -
[The Diana Initiative - \(12:30-12:40 PDT\)](#) - [BBWIC Foundation Tour](#) -
[The Diana Initiative - \(12:40-12:50 PDT\)](#) - [AI Village Tour](#) -
[The Diana Initiative - \(12:50-12:59 PDT\)](#) - [Blacks In Cyber Village Tour](#) -
[The Diana Initiative - The Diana Initiative - Open time](#) -
[Voting Village - cont...\(10:00-17:59 PDT\)](#) - [Voting Village Lab](#) -
[Voting Village - Keynote: Colorado's Creation of RLAs](#) - Wayne Williams

[Adversary Village](#) - (13:30-13:59 PDT) - [Field Notes on Offensive Agents: Reusability, Reliability, and What Breaks](#) - Dominika Pietrzak,Ibai Castells

[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Drone Hacking Workshop](#) -

[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Mission: Compromised - Hacking a Satellite from the Ground Up](#) -

[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Drone Hacking Choose your Own Adventure](#) -

[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Flight Simulator/EFB](#) -

[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [MOUSE Runner & Flappy Drone](#) -

[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Satellites Under Attack: Hands-On Satellite Security Threat Scenarios](#) -

[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Nebula Showdown: Space Systems Security CTF Adventure](#) -

[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [SR-71 Blackbird Badge Challenge](#) -

[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [SpaceCOP - Catch Me If You Can](#) -

[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [DCNextGen - Bricks in the Air](#) -

[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [DCNextGen - RIC-1: ELT Localization Exercise - N3VR-G0N Down](#) -

[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [DCNextGen - Space Grand Challenge - SatHack: The MOUSE-1 Mission](#) -

[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Bricks in the Air](#) -

[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Aerospace Ecosystem Resilience Innovation Environment \(AERIE\) Cyber Range](#) -

[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [ARINC 664 CTF Challenge](#) -

[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Aviation ISAC Cybersecurity Challenge](#) -

[AI Village](#) - cont...(10:00-17:59 PDT) - [AI Village: Village Open](#) -

[AI Village](#) - cont...(10:00-17:59 PDT) - [Poster Presentations](#) -

[AI Village](#) - cont...(10:00-17:59 PDT) - [Cyber Mirage: Realtime Deepfake Demos](#) - Brandon Kovacs

[AppSec Village](#) - cont...(12:45-13:45 PDT) - [OWASP FinBot CTF: Hands-On Agentic AI Threats](#) - Helen Oakley,saikishu

[AppSec Village](#) - (13:15-15:59 PDT) - [Supply Chain Isn't Just Dependencies Anymore: Defending Developers, Tooling, and Builds](#) - Tanya "SheHacksPurple" Janca

[AppSec Village](#) - (13:30-13:59 PDT) - [How Shadow APIs Become an Attacker's Free Pass Into Your Cloud-Native App](#) - Emma Yuan Fang,Krity

[AppSec Village](#) - [Code Invaders: Stop The Insecure Code](#) - Mackenzie

[AppSec Village](#) - [AppSec Quiz Gauntlet: Spot the Vulnerability](#) - Avek Kolech

[AppSec Village](#) - [AI Pentesting Trivia Showdown](#) - Andy Dennis,Bill Reyor

[AppSec Village](#) - [Factory Floor MVP Incident Response Challenge](#) -

[Biohacking Village](#) - cont...(10:00-17:59 PDT) - [Embedded & Shredded: Advanced Embedded System Hacking](#) -

[Biohacking Village](#) - cont...(10:00-17:59 PDT) - [Biohacking Device Lab](#) -

[Biohacking Village](#) - [Safe, Secure, and Effective: What Static Behavior Analysis Reveals About the Software Running Your Medical Devices](#) - Andrew Hendela

[Blacks In Cyber Village](#) - [Bias is a Bug: Why Inequality is a Cybersecurity Vulnerability](#) - Dr. Fatou Sankare

[Blue Team Village](#) - (13:15-14:15 PDT) - [Threat Intelligence in Real Life](#) - Ashley Sequeira,Julian Zottl,Leigh Gilbert,Madeline Sedgwick

[Bug Bounty Village](#) - cont...(12:30-13:30 PDT) - [Better Bug Hunting on AI Products: A VRP Lead's Perspective](#) - John Kotheimer

[Call Center Village](#) - cont...(10:00-17:59 PDT) - [Call Center Village - Open](#) -

[Car Hacking Village](#) - cont...(10:00-16:59 PDT) - [Bomb Bot Challenge](#) -

[Car Hacking Village](#) - cont...(10:00-17:59 PDT) - [Car Hacking Village Open](#) -

[Cloud Village](#) - (13:30-14:30 PDT) - [Breaking AWS Bedrock: Novel Attack Techniques Against Cloud Infrastructure](#) - Tal Peleg,Maya Parizer

[Cloud Village](#) - (13:30-14:30 PDT) - [Fix It, Snooze It, or Ignore It? Cloud Security Decisions Under Pressure](#) - Mackenzie Jackson

[Cloud Village](#) - [Minimal by Design: Building Hardened Near-Zero-CVE Container Images](#) - Kyle Quest,Ritvik Arya

[Cloud Village](#) - (13:30-14:10 PDT) - [What's Behind the Curtain? Tearing Down AWS's AI Agent Runtime From the Inside](#) - Dan Gansel

[CodeBloom](#) - [What is AI?](#) - Sam Mosley

[Contests - Crash and Compile - Stage Competition -](#)
[Contests - cont...\(10:00-17:59 PDT\) - 5N4CK3Y -](#)
[Contests - cont...\(10:00-17:59 PDT\) - DC's Next Top Threat Model -](#)
[Contests - cont...\(10:00-17:59 PDT\) - Untechnical -](#)
[Contests - cont...\(10:00-17:59 PDT\) - DEF CON Scavenger Hunt -](#)
[Contests - cont...\(10:00-17:59 PDT\) - Darknet-NG -](#)
[Contests - cont...\(10:00-17:59 PDT\) - Crack Me If You Can 2026 -](#)
[Contests - cont...\(10:00-17:59 PDT\) - TeleChallenge -](#)
[Contests - cont...\(10:00-17:59 PDT\) - HackFortress -](#)
[Contests - cont...\(10:00-17:59 PDT\) - ?Cube -](#)
[Contests - cont...\(10:00-17:59 PDT\) - \\$unLight Sh4d0w5 -](#)
[Contests - cont...\(10:00-17:59 PDT\) - Octopus Game - Booth Open -](#)
[Contests - Octopus Game - Walk-In Registration \(Pre-Registration Check-In Closed\) -](#)
[Contests - Octopus Game - Booth Battle #3: The Marbles Match -](#)
[Contests - cont...\(10:00-17:59 PDT\) - Beer Chilling Contraption Contest -](#)
[Contests - cont...\(10:00-17:59 PDT\) - Cryptid Hunt -](#)
[Contests - cont...\(10:00-17:59 PDT\) - HSPACE: AI Battlegrounds -](#)
[Contests - cont...\(10:00-17:59 PDT\) - spyVspy 3: Rat Race -](#)
[Contests - cont...\(10:00-17:59 PDT\) - Hacker Games -](#)
[Contests - cont...\(10:00-17:59 PDT\) - PhreakMe -](#)
[Contests - cont...\(10:00-17:59 PDT\) - Game Hacking Village CTF -](#)
[Contests - cont...\(10:00-17:59 PDT\) - Kubernetes CTF -](#)
[Contests - cont...\(10:00-17:59 PDT\) - Hac-Man -](#)
[Contests - cont...\(10:00-17:59 PDT\) - Crack the Core -](#)
[Contests - cont...\(10:00-17:59 PDT\) - Cyber Deck Competition -](#)
[Contests - cont...\(10:00-17:59 PDT\) - Pinball High Score Contest -](#)
[Contests - cont...\(10:00-17:59 PDT\) - Code Cadaver: Break Every System. Save Your Friend. -](#)
[Contests - cont...\(10:00-17:59 PDT\) - PWN UR H0M3 - DDoS CTF -](#)
[Contests - cont...\(10:00-17:59 PDT\) - Reali7y Overrun - Contest running -](#)
[Contests - cont...\(10:00-17:59 PDT\) - Tin Foil Hat Contest -](#)
[Contests - cont...\(10:00-17:59 PDT\) - CMD+CTRL Cyber Range: DarkMoney -](#)
[Contests - cont...\(12:00-14:59 PDT\) - Dozier Drill Tournament -](#)
[Contests - Locktopus - Semi Finals -](#)
[Contests - cont...\(10:00-17:59 PDT\) - Radio Frequency Capture the Flag -](#)
[Contests - cont...\(10:00-17:59 PDT\) - DEF CON CTF: Benevolent Bureau of Birds -](#)
[Contests - cont...\(10:00-17:59 PDT\) - AI Village - Hal CTF -](#)
[Contests - cont...\(10:00-17:59 PDT\) - AI Village Plays Pokemon: DEFCON Edition - Nick Ashworth](#)
[Contests - cont...\(10:00-16:59 PDT\) - Car Hacking Village CTF -](#)
[Contests - cont...\(12:00-15:59 PDT\) - Global OSINT Search Party CTF – DEF CON 34 Edition -](#)
[Contests - cont...\(10:00-17:59 PDT\) - OWASP CTF -](#)
[Contests - cont...\(10:00-17:59 PDT\) - Escalation Desk CTF -](#)
[Contests - cont...\(10:00-17:59 PDT\) - DEF CON Groups Backdoors & Breaches - Tim Doerges,Seth Benning](#)
[Contests - cont...\(10:00-17:59 PDT\) - DEF CON Groups Sticker Contest -](#)
[Contests - cont...\(10:00-23:59 PDT\) - Apex Park \(Cloud Village CTF\) -](#)
[Contests - cont...\(10:00-17:59 PDT\) - Hacking GRC Contest -](#)
[Cryptocurrency Village - Evading LLM Detection - Hanley Shun,Cong Zhang,; Oscar Skjerven](#)
[Data Duplication Village - cont...\(10:00-17:59 PDT\) - DDV open and accepting drives for duplication -](#)
[Data Duplication Village - Drive Stats: 14 years of hard drive failure rates - Stephanie Doyle](#)
[DCNextGen - Hacker Culture 101 - medus4](#)
[DEF CON Groups - Building a Strong Community Culture presented by DC407 - Edna Jonsson,Dustin](#)
[DEF CON Groups - cont...\(10:00-17:59 PDT\) - DEF CON Groups \(DCG\) -](#)
[DEF CON Talks - gpwn: Wiretapping fiber \(GPON\) ISP deployments from the comfort of your home - Rithwik "the131"](#)
[Jayasimha,Rithvik Vibhu](#)
[DEF CON Talks - cont...\(12:30-13:30 PDT\) - Writing to Shadow Stacks - Vladimir "G1ND1L4" Tokarev](#)
[DEF CON Talks - \(13:30-14:30 PDT\) - Bring Your Own Root Of Trust - Mickey "@HackingThings" Shkatov,Jesse Michael](#)

DEF CON Talks - [Stalking the Wily Hacker ... 40 years later](#) - Cliff Stoll

DEF CON Talks - cont...(12:30-13:30 PDT) - [Compounding Interest: Exploiting the ATM Supply Chain](#) - Matt Burch

DEF CON Talks - (13:30-14:30 PDT) - [Transformers: Dark Side of the Type - Weaponizing the Conversion Layer](#) - Oleksandr Miros

DEF CON Talks - [Dylib Hijacking on macOS: Dead or Alive?](#) - Patrick Wardle

DEF CON Training - cont...(08:30-17:30 PDT) - [Blue vs Red Bootcamp: From Attacker Playbooks to Defender Detections](#) - Carlo Anez Mazurco, Mariana Ruiz

DEF CON Training - cont...(08:30-17:30 PDT) - [Influence Operations: Tactics, Defense, and Exploitation](#) - Greg Conti, Tom Cross

DEF CON Training - cont...(08:30-17:30 PDT) - [Full-Stack Pentesting Laboratory: 100% Hands-On + Lifetime LAB Access](#) - Dawid Czagan

Demo Labs - [AD-Necromancer: Resurrecting Forgotten Control Paths in Active Directory](#) - Akbar "0xsensei" Abdullayev, 0xHera

Demo Labs - [MalSkill Lab: Hands-On Natural Language Malware in AI Agent Orchestration Systems](#) - Nur "BurritoTheNurrito" Gucu

Demo Labs - [Keychecker : SSH Key based attack tool for DVCS Systems](#) - Anant Shrivastava

Demo Labs - [Hook Crook - Extracting More From Discord Webhooks](#) - Jeremy Banker - K0JLB, Arity0

Demo Labs - [L.A.Y.E.R.S - Layered Analysis Engine for Browser Extension Risk and Security](#) - Abhinav Khanna, Krishna Chaganti

Demo Labs - [Trajan: Cross-Platform CI/CD Security Scanner](#) - Rahul Saranjame, Ranganatha Rao Sridhar, Tanishq Rupaal

Embedded Systems Village - cont...(10:00-17:59 PDT) - [Embedded - 101 Labs](#) - Embedded Systems Village - cont...(10:00-17:59 PDT) - [Thread Carefully](#) - Embedded Systems Village - cont...(10:00-17:59 PDT) - [Exploit Bluetooth Low Energy with BLESPlloit and optional ESP32](#) - Slawomir Jasek

Embedded Systems Village - cont...(10:00-17:59 PDT) - [Embedded Systems Village CTF](#) - Game Hacking Village - cont...(10:00-15:59 PDT) - [Chill Zone: Casual Games & TASBot Smash Demo](#) - Game Hacking Village - cont...(10:00-16:59 PDT) - [Riot Games Vanguard: Pwn to own](#) - Ham Radio Village - [Why Signals Still Matter: Amateur Radio in the Age of Cell Phones](#) - Nate Moore

IoT Village - cont...(10:00-17:59 PDT) - [Expose Hidden Surveillance in Everyday Tech](#) - IoT Village - cont...(10:00-17:59 PDT) - [Smart Home in the Matter: Blink, Race, Attack CTF](#) - IoT Village - cont...(10:00-17:59 PDT) - [Discover GE Appliances!](#) - IoT Village - cont...(10:00-17:59 PDT) - [All About UART](#) - IoT Village - cont...(10:00-17:59 PDT) - [Hands-On Hardware Hacking – From JTAG to Root, Memory Patching Boot Process for Root Access](#) - IoT Village - cont...(10:00-17:59 PDT) - [Just Hacking Training](#) - IoT Village - cont...(10:00-17:59 PDT) - [Raiders of the Lost Firmware: A Hands-On Workshop in IoT Firmware Archaeology](#) - IoT Village - cont...(10:00-17:59 PDT) - [Cat-astrophic Hacking: Breaking Into Smart Litter Boxes](#) - IoT Village - cont...(12:00-13:30 PDT) - [Wi-Fi Self Defense & Hacker Hunting & For Beginners](#) - Kody Kinzie

IoT Village - cont...(12:30-13:30 PDT) - [Raiders of the Lost Firmware: A Hands-On Workshop in IoT Firmware Archaeology](#) - Simone Bossi, Luca Borzacchiello

La Villa Community - cont...(12:30-13:30 PDT) - [Descubrimiento Industrializado de CVEs con Agentes de IA](#) - Simon Correa, Michael Rivera

La Villa Community - (13:30-13:59 PDT) - [The CVE-Hunters Project: From Noobs to Researchers](#) - Natan Morette

Lonely Hackers Club - cont...(10:00-17:59 PDT) - [Lonely Hackers Club - Lockpicking Table](#) - Lonely Hackers Club - cont...(10:00-17:59 PDT) - [Lonely Hackers Club CTF](#) - Lonely Hackers Club - cont...(10:00-17:59 PDT) - [Lonely Hackers Club - Sticker Swap Table](#) - Lonely Hackers Club - cont...(10:30-16:30 PDT) - [Resume Review with the Lonely Hackers Club](#) - Maker's Village - cont...(10:00-17:59 PDT) - [Makers' Village - Hacker Arts and Crafts](#) - Maker's Village - [Crafting the Future: DEF CON 34 Light-Up Bow Workshop](#) - Malware Village - [Ropkit: Framework for Windows Kernel Code Execution under HVCI](#) - Nathan Sawyer

Malware Village - (13:50-14:30 PDT) - [How to destroy a country](#) - Lisandro Ubiedo, Leandro Cuozzo

Malware Village - cont...(12:55-14:05 PDT) - [A hands-on hour with IDA: reverse-engineer a real DLL-sideload attack from safe, purpose-built samples. No experience required — you'll crack your first binary in the first ten minutes.](#) - David Rushmer

Middle Easterns & Africans in Cyber Security (MEACS) - BewAIre: Detecting Malicious Pull Requests at Scale with LLMs - Andrew Krug
 Misc - (13:30-14:30 PDT) - Why Mandatory Age Verification Keeps Us All Less Safe - Alexis Hancock,Kenyatta Thomas
 Mobile Hacking Community - cont...(10:00-17:59 PDT) - Mobile Hacking Community - Open -
 Mobile Hacking Community - cont...(10:00-17:59 PDT) - Mobile Hacking - Informal CTF -
 Mobile Hacking Community - (13:15-14:45 PDT) - Hacking iOS Apps in a Structured Way - Sven Schleier
 Nix Vegas Community - Whose PR Is It Anyway? -
 Noob Community - cont...(10:00-17:59 PDT) - Skillbit Labs -
 Noob Community - cont...(10:00-17:59 PDT) - No Stupid Questions -
 Noob Community - cont...(10:00-17:59 PDT) - TCM Security Labs -
 Noob Community - cont...(10:00-17:59 PDT) - SANS Institute NetWars Labs -
 Noob Community - cont...(10:00-17:59 PDT) - Mentoring and Career Advice -
 Noob Community - cont...(10:00-17:59 PDT) - Hack The Box DC Junior Ranger Program Challenge -
 Noob Community - cont...(10:00-17:59 PDT) - Arcanum Security Labs -
 Noob Community - cont...(10:00-17:59 PDT) - Kryptsec Labs -
 Noob Community - redStack: Boot-to-Breach Red Team Platform - Michael Ortiz
 Noob Community - Getting Started in OT/ICS Cybersecurity - Mike Holcomb
 OSINT For Good Community - cont...(10:00-17:59 PDT) - OSINT4Good Community - DC NextGen Content -
 OSINT For Good Community - cont...(10:00-17:59 PDT) - FINDX OSINT Educational Series -
 OWASP Foundation - cont...(10:00-17:59 PDT) - BadVR: Signals Everywhere a collaboration with XR Village - Jad Meouchy,Suzanne Borders
 OWASP Foundation - FTS Build it Yourself: cDc X OWASP X Veilid - Gibson,medus4,cdC & Veilid crew
 Packet Hacking Village - Building Better Backdoors Than China - Khael Kugler
 Physical Security Village - (13:30-13:59 PDT) - FORTRESS Framework - Brad "Sno0ose" Ammerman
 Policy @ DEF CON - cont...(12:30-13:30 PDT) - Privacy You Inherit: How Cultural History Writes the Source Code for AI Surveillance Policy - Tati
 Policy @ DEF CON - (13:30-13:59 PDT) - The Subverted Hacker - Robert "zizkill" Shala
 Policy @ DEF CON - Surprise Session - Check Hacker Tracker -
 Queercon Community - Ace/Aro Meetup -
 Radio Frequency Village - cont...(10:00-17:59 PDT) - Radio Frequency Village Events -
 Radio Frequency Village - cont...(12:30-13:25 PDT) - Neotropolis: The Making of the Railgun Trackers - John O'Connor
 Radio Frequency Village - (13:30-13:55 PDT) - This is a Test: Vibe Hacking LTE Cell Broadcast for Emergency Alert Injection - XtraRaj
 Recon Village - cont...(11:00-16:59 PDT) - GE(O)SINT Contest -
 Recon Village - cont...(12:00-13:59 PDT) - Live Recon Contest -
 Recon Village - cont...(12:00-17:59 PDT) - TrackTheFugitive Contest -
 Recon Village - cont...(12:40-15:10 PDT) - The Hard Part of ASM: Ownership Attribution - Jeff Foley
 Recon Village - Tag, You're It: Physical Tracking Tech, Defense, and How to DIY Your Own - Eddie Miro
 Recon Village - (13:30-13:59 PDT) - Your OpSec Is Showing - Fae Blu3Bird" Carlisle
 Red Team Village - cont...(12:00-13:59 PDT) - Ouroboros Attack! Recursive AI-Assisted 0-Day Hunting - Mehmet Önder Key,Temel Demir
 Red Team Village - cont...(12:00-13:59 PDT) - Command & Conquer: Hands-on C2 Primer with Mythic - Logan MacLaren
 Red Team Village - cont...(12:00-13:59 PDT) - Building Hackbots - Jason "jhaddix" Haddix,Ryan Bonner
 Red Team Village - cont...(12:00-13:59 PDT) - Red Teaming Kubernetes: From App-Level CVEs to Full Cluster Takeover - Lenin Alevski
 Red Team Village - You Can't Block My C2 — It's Your Google Calendar - Nishant Tayade
 Red Team Village - Stop Chasing Domain Admin: Designing Red Team Exercises That Matter - Billy Giles
 Scambait Village - cont...(10:00-17:59 PDT) - KSCM Scambait Radio -
 Scambait Village - cont...(10:00-17:59 PDT) - Open Q&A -
 Scambait Village - cont...(12:30-13:59 PDT) - Scammers Don't Discriminate - DolphinVG
 Social Engineering Community Village - cont...(10:00-17:59 PDT) - Social Engineering Community Village - Open Hours -
 Social Engineering Community Village - cont...(10:15-13:15 PDT) - Battle of the Bots: Vishing Edition -
 Social Engineering Community Village - (13:30-14:59 PDT) - Hook, Line & Pretext Workshop: Crafting Effective Phish - Jenn,JC
 Social Gatherings/Events - cont...(09:00-18:59 PDT) - Human Registration Open -

[Social Gatherings/Events - Book Signing - Cindy Cohn](#) - Cindy Cohn
[Social Gatherings/Events - Book Signing - Christopher DeCarmen](#) - Christopher DeCarmen
[Social Gatherings/Events - cont...\(09:00-15:59 PDT\) - Merch \(formerly swag\) Area Open -- README](#) -
[Social Gatherings/Events - cont...\(10:00-18:59 PDT\) - Music - SomaFM](#) -
[Social Gatherings/Events - cont...\(11:00-16:59 PDT\) - Free Ham Radio License Exams](#) -
[The Diana Initiative - Recon Village Tour](#) -
[The Diana Initiative - Voting Village Tour](#) -
[The Diana Initiative - \(13:20-13:30 PDT\) - Hackers with Disabilities Tour](#) -
[The Diana Initiative - \(13:30-13:40 PDT\) - Red Team Village Tour](#) -
[The Diana Initiative - \(13:40-13:50 PDT\) - Scambait Community Tour](#) -
[The Diana Initiative - \(13:50-13:59 PDT\) - Badgelife Tour](#) -
[The Diana Initiative - Everything I Need to Know About Security, I Learned from Mr. Rogers](#) - Zoe
[Voting Village - cont...\(10:00-17:59 PDT\) - Voting Village Lab](#) -
[Voting Village - \(13:30-13:59 PDT\) - Pulling Back the Curtain on the Voting Booth](#) - Marilyn Marks,Max Springer

[Adversary Village](#) - [Microsoft and Amazon are my Favorite C2 Providers](#) - Robert Pimentel

[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [SR-71 Blackbird Badge Challenge](#) -

[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Satellites Under Attack: Hands-On Satellite Security Threat Scenarios](#) -

[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Nebula Showdown: Space Systems Security CTF Adventure](#) -

[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [SpaceCOP - Catch Me If You Can](#) -

[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Drone Hacking Choose your Own Adventure](#) -

[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Drone Hacking Workshop](#) -

[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Flight Simulator/EFB](#) -

[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [MOUSE Runner & Flappy Drone](#) -

[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Mission: Compromised - Hacking a Satellite from the Ground Up](#) -

[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [ARINC 664 CTF Challenge](#) -

[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Aerospace Ecosystem Resilience Innovation Environment \(AERIE\) Cyber Range](#) -

[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Aviation ISAC Cybersecurity Challenge](#) -

[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Bricks in the Air](#) -

[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [DCNextGen - RIC-1: ELT Localization Exercise - N3VR-G0N Down](#) -

[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [DCNextGen - Space Grand Challenge - SatHack: The MOUSE-1 Mission](#) -

[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [DCNextGen - Bricks in the Air](#) -

[Aerospace Village](#) - [Racing PX4: Memory Safety and Timing Vulnerabilities](#) - Nefeli Georgilas

[Aerospace Village](#) - (14:30-14:59 PDT) - [Hacking AFDX or Not; A Primer for Flight Control Systems Security](#) - Andrew Tierney,Adam Bromiley

[AI Village](#) - cont...(10:00-17:59 PDT) - [Poster Presentations](#) -

[AI Village](#) - cont...(10:00-17:59 PDT) - [Cyber Mirage: Realtime Deepfake Demos](#) - Brandon Kovacs

[AI Village](#) - cont...(10:00-17:59 PDT) - [AI Village: Village Open](#) -

[AI Village](#) - [The Agentic Free Pass: Does an Abliterated Backbone Make Agents Easier to Attack?](#) - Karol Piekarski,Nishith Sinha

[AI Village](#) - [What we learned from SATAN about the MYTH of Mythos](#) - Jeff Crume

[AI Village](#) - (14:30-14:59 PDT) - [That's Not Your Agent: Why Zero Trust Can't Tell](#) - Kriti Kharbanda,Emma Yuan Fang

[AppSec Village](#) - [OWASP AIBOM Generator](#) - Dmitry Raidman,Helen Oakley

[AppSec Village](#) - cont...(13:15-15:59 PDT) - [Supply Chain Isn't Just Dependencies Anymore: Defending Developers, Tooling, and Builds](#) - Tanya "SheHacksPurple" Janca

[AppSec Village](#) - [Every ride you take - Hacking a City's Public Transportation](#) - Ignacio Navarro

[AppSec Village](#) - (14:50-15:20 PDT) - [Pattern, Graph, Prompt: What Happens When You Layer Three Analysis Paradigms on the Same Codebase](#) - Mudita Khurana

[AppSec Village](#) - cont...(13:00-14:59 PDT) - [Code Invaders: Stop The Insecure Code](#) - Mackenzie

[AppSec Village](#) - cont...(13:00-14:59 PDT) - [AppSec Quiz Gauntlet: Spot the Vulnerability](#) - Avek Kolech

[AppSec Village](#) - cont...(13:00-14:59 PDT) - [AI Pentesting Trivia Showdown](#) - Andy Dennis,Bill Reyor

[AppSec Village](#) - cont...(13:00-14:59 PDT) - [Factory Floor MVP Incident Response Challenge](#) -

[Biohacking Village](#) - cont...(10:00-17:59 PDT) - [Biohacking Device Lab](#) -

[Biohacking Village](#) - cont...(10:00-17:59 PDT) - [Embedded & Shredded: Advanced Embedded System Hacking](#) -

[Blacks In Cyber Village](#) - [Exploring Security Features in the Armv8-M Architecture](#) - Ian Harris,Jacob Gutierrez

[Blue Team Village](#) - cont...(13:15-14:15 PDT) - [Threat Intelligence in Real Life](#) - Ashley Sequeira,Julian Zottl,Leigh Gilbert,Madeline Sedgwick

[Blue Team Village](#) - (14:30-15:30 PDT) - [AI Security: Hype, Hacks, and the Future of Defense](#) - Karan Dwivedi,Thomas Roccia,Todd Fletcher

[Bug Bounty Village](#) - [Exfil Everything: A Year of Stealing Data from AI Agents](#) - Ads Dawson,Mike "TakSec" Takahashi

[Bug Bounty Village](#) - (14:30-15:59 PDT) - [Bots, Bounties, and Bullshit: An Honest Panel on AI in Hacking](#) - Ben "NahamSec" Sadeghipour,Vitor "busf4ctor" Falcao Habibe Costa,Joey Melo,Dustin "ph1r3574r73r" Farley,Ads Dawson,Johann "wunderwuzzi23" Rehberger

[Call Center Village](#) - cont...(10:00-17:59 PDT) - [Call Center Village - Open](#) -

[Car Hacking Village](#) - cont...(10:00-16:59 PDT) - [Bomb Bot Challenge](#) -

[Car Hacking Village](#) - cont...(10:00-17:59 PDT) - [Car Hacking Village Open](#) -
[Cloud Village](#) - cont...(13:30-14:30 PDT) - [Breaking AWS Bedrock: Novel Attack Techniques Against Cloud Infrastructure](#) -
 Tal Peleg, Maya Parizer
[Cloud Village](#) - cont...(13:30-14:30 PDT) - [Fix It, Snooze It, or Ignore It? Cloud Security Decisions Under Pressure](#) -
 Mackenzie Jackson
[Cloud Village](#) - cont...(13:30-14:10 PDT) - [What's Behind the Curtain? Tearing Down AWS's AI Agent Runtime From the Inside](#) -
 Dan Gansel
[Cloud Village](#) - [Autonomous Offense vs. Autonomous Defense: Who's Winning in the Cloud?](#) -
[Cloud Village](#) - (14:50-15:20 PDT) - [cloud-auth: a provider-agnostic CLI for cross-cloud workload identity](#) - Aniruddha Biyani
[CodeBloom](#) - [Work Session: Ciphers](#) -
[Contests](#) - cont...(13:00-14:59 PDT) - [Crash and Compile - Stage Competition](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [5N4CK3Y](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [DC's Next Top Threat Model](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Untechnical](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [DEF CON Scavenger Hunt](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Darknet-NG](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Crack Me If You Can 2026](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [TeleChallenge](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [HackFortress](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [?Cube](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [\\$unLight Sh4d0w5](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Octopus Game - Booth Open](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Beer Chilling Contraption Contest](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Cryptid Hunt](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [HSPACE: AI Battlegrounds](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [spyVspy 3: Rat Race](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Hacker Games](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [PhreakMe](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Game Hacking Village CTF](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Kubernetes CTF](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Hac-Man](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Crack the Core](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Cyber Deck Competition](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Pinball High Score Contest](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Code Cadaver: Break Every System. Save Your Friend.](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [PWN UR H0M3 - DDoS CTF](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Real7y Overrun - Contest running](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Tin Foil Hat Contest](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [CMD+CTRL Cyber Range: DarkMoney](#) -
[Contests](#) - cont...(12:00-14:59 PDT) - [Dozier Drill Tournament](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Radio Frequency Capture the Flag](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [DEF CON CTF: Benevolent Bureau of Birds](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [AI Village - Hal CTF](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [AI Village Plays Pokemon: DEFCON Edition](#) - Nick Ashworth
[Contests](#) - cont...(10:00-16:59 PDT) - [Car Hacking Village CTF](#) -
[Contests](#) - cont...(12:00-15:59 PDT) - [Global OSINT Search Party CTF – DEF CON 34 Edition](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [OWASP CTF](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Escalation Desk CTF](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [DEF CON Groups Backdoors & Breaches](#) - Tim Doerges, Seth Benning
[Contests](#) - cont...(10:00-17:59 PDT) - [DEF CON Groups Sticker Contest](#) -
[Contests](#) - cont...(10:00-23:59 PDT) - [Apex Park \(Cloud Village CTF\)](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Hacking GRC Contest](#) -
[Crypto & Privacy Village](#) - [Forget FIPS: An Analysis of Russian and Chinese Cryptographic Standards](#) - Infocalypse
[Data Duplication Village](#) - cont...(10:00-17:59 PDT) - [DDV open and accepting drives for duplication](#) -

DCNextGen - cont...(13:00-14:15 PDT) - [Hacker Culture 101](#) - medus4

DEF CON Groups - cont...(10:00-17:59 PDT) - [DEF CON Groups \(DCG\)](#) -

DEF CON Talks - [Lights Out: Out-of-Band, Out of Mind, Out of Control](#) - HD "hdm" Moore

DEF CON Talks - cont...(13:30-14:30 PDT) - [Bring Your Own Root Of Trust](#) - Mickey "@HackingThings" Shkatov, Jesse Michael

DEF CON Talks - (14:30-15:30 PDT) - [Bird Hunting Season: The Final Flight](#) - Jon "GainSec" Gaines

DEF CON Talks - [Cracking North Korea's Information Control: How Smugglers, Defectors, and Technologists are Breaking Open the World's Most Locked-Down Information System](#) - JDT

DEF CON Talks - cont...(13:30-14:30 PDT) - [Transformers: Dark Side of the Type - Weaponizing the Conversion Layer](#) - Oleksandr Mirosh

DEF CON Talks - (14:30-15:30 PDT) - [Looking and Peering: Attacking from beyond BGP Adjacency](#) - Bo-Shiun "bronson113" Yen

DEF CON Talks - [The Enclave is Lying to You: Breaking TEE Trust Boundaries Through Boot-Time State](#) - Sandeep "pyro" Jayashankar

DEF CON Training - cont...(08:30-17:30 PDT) - [Blue vs Red Bootcamp: From Attacker Playbooks to Defender Detections](#) - Carlo Anez Mazurco, Mariana Ruiz

DEF CON Training - cont...(08:30-17:30 PDT) - [Influence Operations: Tactics, Defense, and Exploitation](#) - Greg Conti, Tom Cross

DEF CON Training - cont...(08:30-17:30 PDT) - [Full-Stack Pentesting Laboratory: 100% Hands-On + Lifetime LAB Access](#) - Dawid Czagan

DEF CON Workshops - [Sold Out - Hands-on DuckyScript: An Introduction to HID Attack Tools with O.MG Devices](#) - wasabi, Ø1, Tokugero

DEF CON Workshops - [Sold Out - Purple Teaming Industrial Control Systems](#) - Arnaud SOULLIE, Alexandrine Torrents

DEF CON Workshops - [Sold Out - Entra ID Persistence - Because Passwords Were Never the Problem](#) - Raunak "Trouble1" Parmar, Chirag "3xpl01tc0d3r" Savla

DEF CON Workshops - [Sold Out - From Prompt to PWN: Exploiting LLM Powered Web Applications with OWASP Techniques](#) - Abhinav Verma

DEF CON Workshops - [Sold Out - Intro to Writing Windows Malware with Rust!](#) - iDigitalFlame, Daniel Bravo

DEF CON Workshops - [Sold Out - Building Agentic Reverse Engineering "Skills"](#) - John "clearbluejar" McIntosh

DEF CON Workshops - [Sold Out - Learning to Reverse Engineer Compiled C as We Learn to Write It](#) - Wesley McGrew

DEF CON Workshops - [Sold Out - Salesforce Apex Predator: Breaking Salesforce Sites](#) - Nitay Bachrach, Cynthia Ardman

Demo Labs - [LoKi: A LoRa/Meshtastic based implant for Red Teaming](#) - Venky Raju

Demo Labs - [Intercept.js: Runtime-Aware Detection for JavaScript Environments](#) - Rishi Kant

Demo Labs - [Senrigan \(\) x Suzaku \(\) : Threat Hunting & DFIR for AWS — No SIEM, Just Your Laptop](#) - Fukusuke Takahashi, Zach Mathis, Akira Nishikawa

Demo Labs - [Hook Crook - Extracting More From Discord Webhooks](#) - Jeremy Banker - K0JLB, Arity0

Demo Labs - [PromptPwn: Finding and Exploiting AI-Generated Vulnerabilities at Scale](#) - Georgia Weidman

Demo Labs - [MailX-Ray: A TSA X-Ray for Emails — Air-Gapped Safe-Read and Quick Triage in an Ephemeral MicroVM](#) - Uğur "uJohn" Can ATASOY

Embedded Systems Village - cont...(10:00-17:59 PDT) - [Embedded - 101 Labs](#) -

Embedded Systems Village - cont...(10:00-17:59 PDT) - [Exploit Bluetooth Low Energy with BLESPlloit and optional ESP32](#) - Slawomir Jasek

Embedded Systems Village - cont...(10:00-17:59 PDT) - [Thread Carefully](#) -

Embedded Systems Village - cont...(10:00-17:59 PDT) - [Embedded Systems Village CTF](#) -

Game Hacking Village - cont...(10:00-15:59 PDT) - [Chill Zone: Casual Games & TASBot Smash Demo](#) -

Game Hacking Village - cont...(10:00-16:59 PDT) - [Riot Games Vanguard: Pwn to own](#) -

Game Hacking Village - [Catching Cheaters in Super Smash Bros Melee](#) - AltF4

Hackers.town - [Fun with alternative smartphones with The Tech Reclaimers!](#) - Janet Vertesi

Ham Radio Village - (14:30-14:59 PDT) - [Ham Radio - Licensed to Experiment](#) - Dan W0BDP Norte

ICS Village - [OT Round table. Real talk on how to protect your OT spaces](#) - Aaron Crow, Tom VanNorman, Dillon Lee

ICS Village - (14:45-15:30 PDT) - [Give an AI Industrial Protocol Tools and Watch What It Destroys](#) - Malav Vyas, Asher Davila

IoT Village - cont...(10:00-17:59 PDT) - [Smart Home in the Matter: Blink, Race, Attack CTF](#) -

IoT Village - cont...(10:00-17:59 PDT) - [Expose Hidden Surveillance in Everyday Tech](#) -

IoT Village - cont...(10:00-17:59 PDT) - [Discover GE Appliances!](#) -

IoT Village - cont...(10:00-17:59 PDT) - [All About UART](#) -

IoT Village - cont...(10:00-17:59 PDT) - [Hands-On Hardware Hacking – From JTAG to Root, Memory Patching Boot Process for Root Access](#) -

IoT Village - cont...(10:00-17:59 PDT) - [Just Hacking Training](#) -

IoT Village - cont...(10:00-17:59 PDT) - [Cat-apstrophic Hacking: Breaking Into Smart Litter Boxes](#) -

IoT Village - cont...(10:00-17:59 PDT) - [Raiders of the Lost Firmware: A Hands-On Workshop in IoT Firmware Archaeology](#) -

IoT Village - (14:30-15:15 PDT) - [UAIrT: Over The Air UART](#) - Metehan Arslan,Samet Berk Simsek

La Villa Community - [Keep the Model on Course: Agentic LLM Workflows for Reversing](#) - Asher Davila,Lenin Alevski

La Villa Community - (14:30-15:30 PDT) - [When Cash Runs on Windows: A Red Team Look at ATM Attack Surfaces](#) - Gerardo Mejia

La Villa Community - [Execution of modern techniques to start/improve your career in Incident Response](#) - Ashley Hiram Muñoz

Lonely Hackers Club - cont...(10:00-17:59 PDT) - [Lonely Hackers Club - Lockpicking Table](#) -

Lonely Hackers Club - cont...(10:00-17:59 PDT) - [Lonely Hackers Club - Sticker Swap Table](#) -

Lonely Hackers Club - cont...(10:00-17:59 PDT) - [Lonely Hackers Club CTF](#) -

Lonely Hackers Club - cont...(10:30-16:30 PDT) - [Resume Review with the Lonely Hackers Club](#) -

Maker's Village - cont...(10:00-17:59 PDT) - [Makers' Village - Hacker Arts and Crafts](#) -

Maker's Village - (14:15-14:45 PDT) - [Operation Restoration](#) - Cannibal

Malware Village - cont...(13:50-14:30 PDT) - [How to destroy a country](#) - Lisandro Ubiedo,Leandro Cuozzo

Malware Village - (14:40-15:15 PDT) - [The Permanent Threat: Analyzing Aeternum's Blockchain-Based C2 Operations and Communications](#) - Chris Navarrete,Sai Sathvik Ruppa

Malware Village - cont...(12:55-14:05 PDT) - [A hands-on hour with IDA: reverse-engineer a real DLL-sideload attack from safe, purpose-built samples. No experience required — you'll crack your first binary in the first ten minutes.](#) - David Rushmer

Malware Village - [An Intro to Mac Malware Analysis](#) - Patrick Wardle

Middle Easterns & Africans in Cyber Security (MEACS) - (14:30-14:59 PDT) - [Condense Volumes, Connect Dots, Enrich Contexts: Scaling Root Cause Analysis and Automated Troubleshooting with ML](#) - Ezz Tahoun

Middle Easterns & Africans in Cyber Security (MEACS) - [The Hidden Data Supply Chain: How a SaaS Platform Broadcast Credentials and Customer Identities](#) - Sam Jadali

Misc - cont...(13:30-14:30 PDT) - [Why Mandatory Age Verification Keeps Us All Less Safe](#) - Alexis Hancock,Kenyatta Thomas

Mobile Hacking Community - cont...(10:00-17:59 PDT) - [Mobile Hacking Community - Open](#) -

Mobile Hacking Community - cont...(10:00-17:59 PDT) - [Mobile Hacking - Informal CTF](#) -

Mobile Hacking Community - cont...(13:15-14:45 PDT) - [Hacking iOS Apps in a Structured Way](#) - Sven Schleier

Nix Vegas Community - [Nix Knows When the Agent Is Wrong](#) - Jason Odoom

Nix Vegas Community - (14:45-15:15 PDT) - [Securing Nix Builds using microVMs](#) - Tristan Ross

Noob Community - cont...(10:00-17:59 PDT) - [Arcanum Security Labs](#) -

Noob Community - cont...(10:00-17:59 PDT) - [Kryptsec Labs](#) -

Noob Community - cont...(10:00-17:59 PDT) - [Mentoring and Career Advice](#) -

Noob Community - cont...(10:00-17:59 PDT) - [Hack The Box DC Junior Ranger Program Challenge](#) -

Noob Community - cont...(10:00-17:59 PDT) - [Skillbit Labs](#) -

Noob Community - cont...(10:00-17:59 PDT) - [No Stupid Questions](#) -

Noob Community - cont...(10:00-17:59 PDT) - [SANS Institute NetWars Labs](#) -

Noob Community - cont...(10:00-17:59 PDT) - [TCM Security Labs](#) -

Noob Community - cont...(13:00-14:50 PDT) - [redStack: Boot-to-Breach Red Team Platform](#) - Michael Ortiz

Noob Community - (14:15-14:45 PDT) - [Privilege Escalation: Building a Cyber Career with Zero Support](#) - Akanksha Raghvesh

OSINT For Good Community - cont...(10:00-17:59 PDT) - [OSINT4Good Community - DC NextGen Content](#) -

OSINT For Good Community - cont...(10:00-17:59 PDT) - [F1NDX OSINT Educational Series](#) -

OWASP Foundation - cont...(10:00-17:59 PDT) - [BadVR: Signals Everywhere a collaboration with XR Village](#) - Jad Meouchy,Suzanne Borders

OWASP Foundation - [Agents & Exploits: Hacking OWASP VWAD](#) - Philippe "pilvar" Dourassov

Payment Village - [BNPL's Blind Spot: Exploiting Business Logic Flaws in Buy Now Pay Later APIs](#) - Furkan Fatih Demir

Payment Village - (14:30-15:15 PDT) - [Deepfake Detection Through Adversarial Research](#) - Efim Boieru

Physical Security Village - Clone to Pwn: Remote Badge Cloning with the Flipper Zero - Langston Clement,Dan Goga
 Policy @ DEF CON - The best of three bad ideas? Ransomware taxes in lieu of bans or doing nothing - Joe Uchill
 Policy @ DEF CON - (14:30-15:30 PDT) - From Disclosure to Defense: Rebuilding Vulnerability Management for the AI Era
 - Lindsey Cerkovnik,John Banghart,Ben Flatgard,Elizabeth Eigner
 Queercon Community - Own the con -
 Radio Frequency Village - cont...(10:00-17:59 PDT) - Radio Frequency Village Events -
 Radio Frequency Village - RASM: A State Machine Methodology for RF Security Assessment - Smriti Gaba
 Recon Village - cont...(11:00-16:59 PDT) - GE(O)SINT Contest -
 Recon Village - cont...(12:00-17:59 PDT) - TrackTheFugitive Contest -
 Recon Village - cont...(12:40-15:10 PDT) - The Hard Part of ASM: Ownership Attribution - Jeff Foley
 Red Team Village - Crawlee - Improving crawling with an LLM - Daniel Goldberg
 Red Team Village - Living Off Someone Else's Inference - Armend Gashi,Redon Gashi
 Red Team Village - AIMARU C2: The New Era of LotL (MCP AI-Driven C2) - Mario Lobo
 Red Team Village - BloodBash: Lightweight CLI Python BloodHound Alternative - Anthony Russell
 Red Team Village - Turning Keys and Opening Doors: Leveraging AI Hype to Hack Everything - Will Alexander
 Red Team Village - Chaining Credentials Through the AI Infrastructure Nobody Secured - Nathan Keys
 Scambait Village - cont...(10:00-17:59 PDT) - Open Q&A -
 Scambait Village - cont...(10:00-17:59 PDT) - KSCM Scambait Radio -
 Scambait Village - Creator Talk with RinoaPoison & VanHelen - RinoaPoison,VanHelen
 Social Engineering Community Village - cont...(10:00-17:59 PDT) - Social Engineering Community Village - Open Hours -
 Social Engineering Community Village - For Prompt Injection, Press 1: Hacking AI Voice Agents - Willie Zhang
 Social Engineering Community Village - (14:30-14:59 PDT) - The Sherlock Holmes Social Engineering Playbook - Elizabeth Rasnick
 Social Engineering Community Village - cont...(13:30-14:59 PDT) - Hook, Line & Pretext Workshop: Crafting Effective Phish - Jenn,JC
 Social Gatherings/Events - cont...(09:00-18:59 PDT) - Human Registration Open -
 Social Gatherings/Events - Book Signing - Garrett Gee - Garrett Gee
 Social Gatherings/Events - Book Signing - Brandy Smith - Brandy Smith
 Social Gatherings/Events - cont...(09:00-15:59 PDT) - Merch (formerly swag) Area Open -- README -
 Social Gatherings/Events - cont...(10:00-18:59 PDT) - Music - SomaFM -
 Social Gatherings/Events - cont...(11:00-16:59 PDT) - Free Ham Radio License Exams -
 Telecom Village - Signal Hijacked: How Mobile Networks Became Phishing's Most Trusted Delivery Layer - Sindhura Kona
 Telecom Village - (14:15-14:45 PDT) - From Zero-Day to Zero-Hour: Rethinking Telecom Defense for the Frontier AI Era - Arvind Singh
 The Diana Initiative - Illumicon Tour -
 The Diana Initiative - Hacker Book Club meet up -
 Voting Village - cont...(10:00-17:59 PDT) - Voting Village Lab -
 Voting Village - Separating News from Noise - Ryan Murray,Stephen Richter,Nate Young
 Voting Village - (14:30-14:59 PDT) - Dissecting the ICX Frog - Drew Springall

[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Mission: Compromised - Hacking a Satellite from the Ground Up](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Drone Hacking Workshop](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Flight Simulator/EFB](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [MOUSE Runner & Flappy Drone](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Drone Hacking Choose your Own Adventure](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [SR-71 Blackbird Badge Challenge](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Satellites Under Attack: Hands-On Satellite Security Threat Scenarios](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Nebula Showdown: Space Systems Security CTF Adventure](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [SpaceCOP - Catch Me If You Can](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [DCNextGen - Bricks in the Air](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Bricks in the Air](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [DCNextGen - RIC-1: ELT Localization Exercise - N3VR-G0N Down](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [DCNextGen - Space Grand Challenge - SatHack: The MOUSE-1 Mission](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Aviation ISAC Cybersecurity Challenge](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Aerospace Ecosystem Resilience Innovation Environment \(AERIE\) Cyber Range](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [ARINC 664 CTF Challenge](#) -
[AI Village](#) - cont...(10:00-17:59 PDT) - [AI Village: Village Open](#) -
[AI Village](#) - cont...(10:00-17:59 PDT) - [Poster Presentations](#) -
[AI Village](#) - cont...(10:00-17:59 PDT) - [Cyber Mirage: Realtime Deepfake Demos](#) - Brandon Kovacs
[AI Village](#) - [What can those architecting agents learn from national security?](#) - David C Eight
[AppSec Village](#) - (15:15-16:15 PDT) - [Proactive Malicious Package Defense](#) - Darren Meyer
[AppSec Village](#) - cont...(13:15-15:59 PDT) - [Supply Chain Isn't Just Dependencies Anymore: Defending Developers, Tooling, and Builds](#) - Tanya "SheHacksPurple" Janca
[AppSec Village](#) - cont...(14:50-15:20 PDT) - [Pattern, Graph, Prompt: What Happens When You Layer Three Analysis Paradigms on the Same Codebase](#) - Mudita Khurana
[AppSec Village](#) - (15:30-15:59 PDT) - [How Malicious AI Skills Hijack Your Agents](#) - Jenn Gile
[AppSec Village](#) - [SBOM Find the Flaws](#) - Dmitry Raidman
[AppSec Village](#) - [AppSec Quiz Gauntlet: Spot the Vulnerability](#) - Avek Kolech
[AppSec Village](#) - [AI Pentesting Trivia Showdown](#) - Andy Dennis, William Reyor
[AppSec Village](#) - [The Call Stack Experience](#) - Victoria Keeler
[Biohacking Village](#) - cont...(10:00-17:59 PDT) - [Embedded & Shredded: Advanced Embedded System Hacking](#) -
[Biohacking Village](#) - cont...(10:00-17:59 PDT) - [Biohacking Device Lab](#) -
[Biohacking Village](#) - [AIRGAP BREACHED: Monitoring the Ancestral Payload Leaking from the Poles](#) - David J. Castillo-Cornejo
[Biohacking Village](#) - (15:30-15:59 PDT) - [DarkSyringe: Automated poisoning of Clinical AI Assistants Through PDFs \(a physician's point of view\)](#) - Francesco Costa
[Blacks In Cyber Village](#) - [ChronoRoot: Time-Traveling Through Kernel Trust Boundaries](#) - Ahmeen Muhammad, Sydney Johns
[Blue Team Village](#) - cont...(14:30-15:30 PDT) - [AI Security: Hype, Hacks, and the Future of Defense](#) - Karan Dwivedi, Thomas Roccia, Todd Fletcher
[Blue Team Village](#) - (15:45-16:45 PDT) - [Threat Hunting Explained Badly](#) - Alllison Gallo, Brian Baskin, Silas Cutler, Sydney "letswastetime" Marrone
[Bug Bounty Village](#) - cont...(14:30-15:59 PDT) - [Bots, Bounties, and Bullshit: An Honest Panel on AI in Hacking](#) - Ben "NahamSec" Sadeghipour, Vitor "busf4ctor" Falcao Habibe Costa, Joey Melo, Dustin "ph1r3574r73r" Farley, Ads Dawson, Johann "wunderwuzzi23" Rehberger
[Call Center Village](#) - cont...(10:00-17:59 PDT) - [Call Center Village - Open](#) -
[Car Hacking Village](#) - cont...(10:00-17:59 PDT) - [Car Hacking Village Open](#) -
[Car Hacking Village](#) - cont...(10:00-16:59 PDT) - [Bomb Bot Challenge](#) -
[Car Hacking Village](#) - (15:30-15:59 PDT) - [The Compiler Nobody Satisfactorily Tested: Supply-Chain Gaps in EV Charging Firmware](#) - Kangwon Lee

[Cloud Village](#) - cont...(14:50-15:20 PDT) - [cloud-auth: a provider-agnostic CLI for cross-cloud workload identity](#) - Aniruddha Biyani

[Cloud Village](#) - (15:20-15:59 PDT) - [A New Hope for SSRF: Exploiting Credential Relay from APIM to AI Foundry](#) - Marios Gyftos,Chrysostomos Manousis

[CodeBloom](#) - [Game Time: Input, Output, and Variables](#) -

[Contests](#) - cont...(10:00-17:59 PDT) - [5N4CK3Y](#) -

[Contests](#) - cont...(10:00-17:59 PDT) - [DC's Next Top Threat Model](#) -

[Contests](#) - cont...(10:00-17:59 PDT) - [Untechnical](#) -

[Contests](#) - cont...(10:00-17:59 PDT) - [DEF CON Scavenger Hunt](#) -

[Contests](#) - cont...(10:00-17:59 PDT) - [Darknet-NG](#) -

[Contests](#) - cont...(10:00-17:59 PDT) - [Crack Me If You Can 2026](#) -

[Contests](#) - cont...(10:00-17:59 PDT) - [TeleChallenge](#) -

[Contests](#) - cont...(10:00-17:59 PDT) - [HackFortress](#) -

[Contests](#) - cont...(10:00-17:59 PDT) - [?Cube](#) -

[Contests](#) - cont...(10:00-17:59 PDT) - [\\$unLight Sh4d0w5](#) -

[Contests](#) - cont...(10:00-17:59 PDT) - [Octopus Game - Booth Open](#) -

[Contests](#) - cont...(10:00-17:59 PDT) - [Beer Chilling Contraption Contest](#) -

[Contests](#) - cont...(10:00-17:59 PDT) - [Cryptid Hunt](#) -

[Contests](#) - cont...(10:00-17:59 PDT) - [HSPACE: AI Battlegrounds](#) -

[Contests](#) - cont...(10:00-17:59 PDT) - [spyVspy 3: Rat Race](#) -

[Contests](#) - cont...(10:00-17:59 PDT) - [Hacker Games](#) -

[Contests](#) - cont...(10:00-17:59 PDT) - [PhreakMe](#) -

[Contests](#) - cont...(10:00-17:59 PDT) - [Game Hacking Village CTF](#) -

[Contests](#) - cont...(10:00-17:59 PDT) - [Kubernetes CTF](#) -

[Contests](#) - cont...(10:00-17:59 PDT) - [Hac-Man](#) -

[Contests](#) - cont...(10:00-17:59 PDT) - [Crack the Core](#) -

[Contests](#) - cont...(10:00-17:59 PDT) - [Cyber Deck Competition](#) -

[Contests](#) - cont...(10:00-17:59 PDT) - [Pinball High Score Contest](#) -

[Contests](#) - cont...(10:00-17:59 PDT) - [Code Cadaver: Break Every System. Save Your Friend.](#) -

[Contests](#) - cont...(10:00-17:59 PDT) - [PWN UR H0M3 - DDoS CTF](#) -

[Contests](#) - cont...(10:00-17:59 PDT) - [Real7y Overrun - Contest running](#) -

[Contests](#) - cont...(10:00-17:59 PDT) - [Tin Foil Hat Contest](#) -

[Contests](#) - cont...(10:00-17:59 PDT) - [CMD+CTRL Cyber Range: DarkMoney](#) -

[Contests](#) - [Locktopus - Final Championship](#) -

[Contests](#) - (15:30-17:30 PDT) - [Locktopus Challenge Finals](#) -

[Contests](#) - cont...(10:00-17:59 PDT) - [Radio Frequency Capture the Flag](#) -

[Contests](#) - cont...(10:00-17:59 PDT) - [DEF CON CTF: Benevolent Bureau of Birds](#) -

[Contests](#) - cont...(10:00-17:59 PDT) - [AI Village Plays Pokemon: DEFCON Edition](#) - Nick Ashworth

[Contests](#) - cont...(10:00-17:59 PDT) - [AI Village - Hal CTF](#) -

[Contests](#) - cont...(10:00-16:59 PDT) - [Car Hacking Village CTF](#) -

[Contests](#) - cont...(12:00-15:59 PDT) - [Global OSINT Search Party CTF – DEF CON 34 Edition](#) -

[Contests](#) - cont...(10:00-17:59 PDT) - [OWASP CTF](#) -

[Contests](#) - cont...(10:00-17:59 PDT) - [Escalation Desk CTF](#) -

[Contests](#) - cont...(10:00-17:59 PDT) - [DEF CON Groups Backdoors & Breaches](#) - Tim Doerges,Seth Benning

[Contests](#) - cont...(10:00-17:59 PDT) - [DEF CON Groups Sticker Contest](#) -

[Contests](#) - cont...(10:00-23:59 PDT) - [Apex Park \(Cloud Village CTF\)](#) -

[Contests](#) - cont...(10:00-17:59 PDT) - [Hacking GRC Contest](#) -

[Crypto & Privacy Village](#) - [The Agent Long Con: Tricking Agents Out of Their Data](#) - Patrick Walsh

[Data Duplication Village](#) - cont...(10:00-17:59 PDT) - [DDV open and accepting drives for duplication](#) -

[DCNextGen](#) - [AMA with EFF](#) - EFF

[DEF CON Groups](#) - cont...(10:00-17:59 PDT) - [DEF CON Groups \(DCG\)](#) -

[DEF CON Talks](#) - [Throw Out the Alphabet: Token-Based Markov Chains for Password Cracking](#) - Jon "flakpaket" Gorenflo

[DEF CON Talks](#) - cont...(14:30-15:30 PDT) - [Bird Hunting Season: The Final Flight](#) - Jon "GainSec" Gaines

[DEF CON Talks](#) - (15:30-16:30 PDT) - [Zero-Day Provisioning: Chaining TP-Link ZTP Vulnerabilities for Infiltrating Networks](#) - Francesco La Spina,Stanislav Dashevskyi

DEF CON Talks - Smile, you're on camera! Livestreaming from North Korea's IT workers laptop farm - Heiner García, Mauro Eldritch

DEF CON Talks - cont...(14:30-15:30 PDT) - Looking and Peering: Attacking from beyond BGP Adjacency - Bo-Shiun "bronson113" Yen

DEF CON Talks - (15:30-16:30 PDT) - Wrestling with a Python: Escaping Copilot Studio's AI-Guarded Sandbox - Ryan Hausknecht, Simon Maxwell-Stewart

DEF CON Talks - Get Set, Exploit! Unveiling Python Class Pollution In-the-Wild - Gavin Zhong, Zhengyu Liu, Jianjia Yu

DEF CON Training - cont...(08:30-17:30 PDT) - Blue vs Red Bootcamp: From Attacker Playbooks to Defender Detections - Carlo Anez Mazurco, Mariana Ruiz

DEF CON Training - cont...(08:30-17:30 PDT) - Influence Operations: Tactics, Defense, and Exploitation - Greg Conti, Tom Cross

DEF CON Training - cont...(08:30-17:30 PDT) - Full-Stack Pentesting Laboratory: 100% Hands-On + Lifetime LAB Access - Dawid Czagan

DEF CON Workshops - cont...(14:00-17:59 PDT) - Sold Out - Hands-on DuckyScript: An Introduction to HID Attack Tools with O.MG Devices - wasabi, Ø1, Tokugero

DEF CON Workshops - cont...(14:00-17:59 PDT) - Sold Out - Purple Teaming Industrial Control Systems - Arnaud SOULLIE, Alexandrine Torrents

DEF CON Workshops - cont...(14:00-17:59 PDT) - Sold Out - Entra ID Persistence - Because Passwords Were Never the Problem - Raunak "Trouble1" Parmar, Chirag "3xpl01tc0d3r" Savla

DEF CON Workshops - cont...(14:00-17:59 PDT) - Sold Out - From Prompt to PWN: Exploiting LLM Powered Web Applications with OWASP Techniques - Abhinav Verma

DEF CON Workshops - cont...(14:00-17:59 PDT) - Sold Out - Intro to Writing Windows Malware with Rust! - iDigitalFlame, Daniel Bravo

DEF CON Workshops - cont...(14:00-17:59 PDT) - Sold Out - Building Agentic Reverse Engineering "Skills" - John "clearbluejar" McIntosh

DEF CON Workshops - cont...(14:00-17:59 PDT) - Sold Out - Learning to Reverse Engineer Compiled C as We Learn to Write It - Wesley McGrew

DEF CON Workshops - cont...(14:00-17:59 PDT) - Sold Out - Salesforce Apex Predator: Breaking Salesforce Sites - Nitay Bachrach, Cynthia Ardman

Demo Labs - LoKi: A LoRa/Meshtastic based implant for Red Teaming - Venky Raju

Demo Labs - AC Scanner: The Post-Quantum Cryptographic Exposure and CBOM Generator. You Need This! - Anurag Swarnim Yadav, Joseph Wilson

Demo Labs - Be like a BRAT(BLE Recon and Attack Toolkit): Skip the Handshake, Own the Device - Gigi Xiaoqing Liu, Muzzammil Mohammed, Narmina Karimova

Demo Labs - Ghost in the IDE - Venkata Jayaram Yalla, Pardhiv Reddy

Demo Labs - AOBTD: AI One Bites The DAST - Ozgun "ozzy" Kultekin

Demo Labs - AI Pipeline for N-days Weaponization - Andrea Brosio, Arun Nair

Embedded Systems Village - cont...(10:00-17:59 PDT) - Exploit Bluetooth Low Energy with BLESPlloit and optional ESP32 - Slawomir Jasek

Embedded Systems Village - cont...(10:00-17:59 PDT) - Embedded - 101 Labs -

Embedded Systems Village - cont...(10:00-17:59 PDT) - Thread Carefully -

Embedded Systems Village - cont...(10:00-17:59 PDT) - Embedded Systems Village CTF -

Game Hacking Village - cont...(10:00-15:59 PDT) - Chill Zone: Casual Games & TASBot Smash Demo -

Game Hacking Village - cont...(10:00-16:59 PDT) - Riot Games Vanguard: Pwn to own -

Hackers.town - The Enshittified Internet and How We Can All Rewild the Internet - LambdaCalculus

Ham Radio Village - Meshtastic Beasts and Where to Find Them - Scott Thompson

ICS Village - cont...(14:45-15:30 PDT) - Give an AI Industrial Protocol Tools and Watch What It Destroys - Malav Vyas, Asher Davila

IoT Village - cont...(10:00-17:59 PDT) - Raiders of the Lost Firmware: A Hands-On Workshop in IoT Firmware Archaeology -

IoT Village - cont...(10:00-17:59 PDT) - Cat-astrophic Hacking: Breaking Into Smart Litter Boxes -

IoT Village - cont...(10:00-17:59 PDT) - Hands-On Hardware Hacking – From JTAG to Root, Memory Patching Boot Process for Root Access -

IoT Village - cont...(10:00-17:59 PDT) - Just Hacking Training -

IoT Village - cont...(10:00-17:59 PDT) - All About UART -

IoT Village - cont...(10:00-17:59 PDT) - [Smart Home in the Matter: Blink, Race, Attack CTF](#) -

IoT Village - cont...(10:00-17:59 PDT) - [Expose Hidden Surveillance in Everyday Tech](#) -

IoT Village - cont...(10:00-17:59 PDT) - [Discover GE Appliances!](#) -

IoT Village - [Mesh Nets for Hackers: How \(& When\) to use Meshtastic, Meshcore, & Reticulum!](#) - Kody Kinzie

IoT Village - cont...(14:30-15:15 PDT) - [UAIrT: Over The Air UART](#) - Metehan Arslan,Samet Berk Simsek

IoT Village - (15:15-15:59 PDT) - [Beyond Your Bookshelf: Hackable eReaders](#) - Katie Paxton-Fear

La Villa Community - cont...(14:30-15:30 PDT) - [When Cash Runs on Windows: A Red Team Look at ATM Attack Surfaces](#) - Gerardo Mejia

La Villa Community - (15:30-16:30 PDT) - [From Live Malware to Red Team Tradecraft: Process Hollowing in msbuild.exe](#) - Filipi Pires

La Villa Community - cont...(14:00-15:59 PDT) - [Execution of modern techniques to start/improve your career in Incident Response](#) - Ashley Hiram Muñoz

Lockpick Village - [Intro to Lockpicking](#) -

Lonely Hackers Club - cont...(10:00-17:59 PDT) - [Lonely Hackers Club - Lockpicking Table](#) -

Lonely Hackers Club - cont...(10:00-17:59 PDT) - [Lonely Hackers Club - Sticker Swap Table](#) -

Lonely Hackers Club - cont...(10:00-17:59 PDT) - [Lonely Hackers Club CTF](#) -

Lonely Hackers Club - cont...(10:30-16:30 PDT) - [Resume Review with the Lonely Hackers Club](#) -

Maker's Village - cont...(10:00-17:59 PDT) - [Makers' Village - Hacker Arts and Crafts](#) -

Maker's Village - [Cyberdeck Build](#) - Sk!tz0

Malware Village - cont...(14:40-15:15 PDT) - [The Permanent Threat: Analyzing Aeternum's Blockchain-Based C2 Operations and Communications](#) - Chris Navarrete,Sai Sathvik Rupp

Malware Village - (15:20-16:05 PDT) - [Leigh Trinity OTW](#) - Leigh Gilbert

Malware Village - cont...(14:10-16:50 PDT) - [An Intro to Mac Malware Analysis](#) - Patrick Wardle

Middle Easterns & Africans in Cyber Security (MEACS) - [Agents of Chaos: A Field Guide to How Agentic AI Gets Owned, and What Trust Nothing Looks Like in Practice](#) - Amber Bennoui

Misc - (15:30-16:30 PDT) - [Privacy's Defender with Women in Security and Privacy \(WISP\)](#) - Cindy Cohn,Alyssa Coley

Mobile Hacking Community - cont...(10:00-17:59 PDT) - [Mobile Hacking Community - Open](#) -

Mobile Hacking Community - cont...(10:00-17:59 PDT) - [Mobile Hacking - Informal CTF](#) -

Mobile Hacking Community - [Beerus Framework – A New Mobile Framework Arises](#) - João Pedro Tricta,Daniel "Daniboy" França Lima

Nix Vegas Community - cont...(14:45-15:15 PDT) - [Securing Nix Builds using microVMs](#) - Tristan Ross

Nix Vegas Community - (15:30-16:30 PDT) - [Your Infrastructure Is a DAG: Manage It With Nix](#) - Ethan Carter Edwards

Noob Community - cont...(10:00-17:59 PDT) - [TCM Security Labs](#) -

Noob Community - cont...(10:00-17:59 PDT) - [SANS Institute NetWars Labs](#) -

Noob Community - cont...(10:00-17:59 PDT) - [Skillbit Labs](#) -

Noob Community - cont...(10:00-17:59 PDT) - [No Stupid Questions](#) -

Noob Community - cont...(10:00-17:59 PDT) - [Kryptsec Labs](#) -

Noob Community - cont...(10:00-17:59 PDT) - [Arcanum Security Labs](#) -

Noob Community - cont...(10:00-17:59 PDT) - [Mentoring and Career Advice](#) -

Noob Community - cont...(10:00-17:59 PDT) - [Hack The Box DC Junior Ranger Program Challenge](#) -

Noob Community - [Six Impossible Things Before Breakfast: Common Misconceptions About Being a CTI Analyst](#) - Brett Tolbert

Noob Community - [AI Hacking for Noobs](#) - Jason "jhaddix" Haddix,Arcanum Information Security Team

OSINT For Good Community - cont...(10:00-17:59 PDT) - [OSINT4Good Community - DC NextGen Content](#) -

OSINT For Good Community - cont...(10:00-17:59 PDT) - [FINDX OSINT Educational Series](#) -

OWASP Foundation - cont...(10:00-17:59 PDT) - [BadVR: Signals Everywhere a collaboration with XR Village](#) - Jad Meouchy,Suzanne Borders

OWASP Foundation - cont...(14:00-15:59 PDT) - [Agents & Exploits: Hacking OWASP VWAD](#) - Philippe "pilvar" Dourassov

Packet Hacking Village - [There's A Bug in My Boot! Finding Vulnerabilities in U-Boot](#) - Jared Stroud

Payment Village - cont...(14:30-15:15 PDT) - [Deepfake Detection Through Adversarial Research](#) - Efim Boieru

Policy @ DEF CON - cont...(14:30-15:30 PDT) - [From Disclosure to Defense: Rebuilding Vulnerability Management for the AI Era](#) - Lindsey Cerkovnik,John Banghart,Ben Flatgard,Elizabeth Eigner

Policy @ DEF CON - (15:30-15:59 PDT) - [Assume Breach, But For Real: Rewriting Infrastructure Policy for the Adversaries Who Never Left](#) - Travis Berent,Adam Hickey

Queercon Community - [Men Loving Men Meetup](#) -

Radio Frequency Village - cont...(10:00-17:59 PDT) - Radio Frequency Village Events -
Radio Frequency Village - Drone ID on the Wire: RF Detection, Spoofing, and the Limits of Compliance-Based Airspace Awareness - Greg Albrecht
Recon Village - cont...(11:00-16:59 PDT) - GE(O)SINT Contest -
Recon Village - cont...(12:00-17:59 PDT) - TrackTheFugitive Contest -
Recon Village - cont...(12:40-15:10 PDT) - The Hard Part of ASM: Ownership Attribution - Jeff Foley
Recon Village - (15:20-17:50 PDT) - Vibe Coding Your Way to a Fully Functional Open-Source Intelligence Platform - Lenin Alevski
Recon Village - The Breach Is Over. The Exposure Is Not - Kumar Ashwin,Anant Shrivastava
Recon Village - (15:30-15:59 PDT) - Cl0p ^_- Til You Drop - 6 years, 9 Campaigns, 7 0-Days - Eli Woodward
Red Team Village - cont...(14:00-15:59 PDT) - Crawlee - Improving crawling with an LLM - Daniel Goldberg
Red Team Village - cont...(14:00-15:59 PDT) - Living Off Someone Else's Inference - Armend Gashi,Redon Gashi
Red Team Village - cont...(14:00-15:59 PDT) - AIMARU C2: The New Era of LotL (MCP AI-Driven C2) - Mario Lobo
Red Team Village - cont...(14:00-15:59 PDT) - BloodBash: Lightweight CLI Python BloodHound Alternative - Anthony Russell
Red Team Village - Requiem for the Decommissioned: When Dead Hosts Bite Back - Yekaterina Shevchenko
Red Team Village - Breaking MCP Trust Boundaries: Cross-Server Authority Injection in Agent Toolchains - Yevhen Pervushyn
Scambait Village - cont...(10:00-17:59 PDT) - Open Q&A -
Scambait Village - cont...(10:00-17:59 PDT) - KSCM Scambait Radio -
Scambait Village - cont...(14:00-15:30 PDT) - Creator Talk with RinoaPoison & VanHelen - RinoaPoison,VanHelen
Scambait Village - (15:30-16:59 PDT) - Creator Drop-In -
Social Engineering Community Village - cont...(10:00-17:59 PDT) - Social Engineering Community Village - Open Hours -
Social Engineering Community Village - A Framework for Evaluating AI-Enabled Social Engineering - Fred Heiding
Social Engineering Community Village - (15:30-15:59 PDT) - What Scammers Know That Social Engineers Don't: Three Techniques for Tough Cases - Megan Squire
Social Engineering Community Village - (15:30-17:30 PDT) - 2027 SECVC Pre-Qualification Round - JC,Snow
Social Gatherings/Events - cont...(09:00-18:59 PDT) - Human Registration Open -
Social Gatherings/Events - Book Signing - Mark Foudy - Mark Foudy
Social Gatherings/Events - cont...(09:00-15:59 PDT) - Merch (formerly swag) Area Open -- README -
Social Gatherings/Events - cont...(10:00-18:59 PDT) - Music - SomaFM -
Social Gatherings/Events - cont...(11:00-16:59 PDT) - Free Ham Radio License Exams -
Social Gatherings/Events - DCG New England Meetup -
Telecom Village - (15:45-16:45 PDT) - Industry Challenges & SOC Reality - Vinod Shrimali
The Diana Initiative - cont...(14:00-15:59 PDT) - Hacker Book Club meet up -
Voting Village - cont...(10:00-17:59 PDT) - Voting Village Lab -
Voting Village - (15:30-15:59 PDT) - Alerts and Warnings in 2026 Elections - Geoff Hale,Ryan Macias

[Return to Index](#) - [Locations Legend](#)

[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [SR-71 Blackbird Badge Challenge](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Nebula Showdown: Space Systems Security CTF Adventure](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [SpaceCOP - Catch Me If You Can](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Satellites Under Attack: Hands-On Satellite Security Threat Scenarios](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Drone Hacking Workshop](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Flight Simulator/EFB](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [MOUSE Runner & Flappy Drone](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Drone Hacking Choose your Own Adventure](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Mission: Compromised - Hacking a Satellite from the Ground Up](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Aerospace Ecosystem Resilience Innovation Environment \(AERIE\) Cyber Range](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Aviation ISAC Cybersecurity Challenge](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [ARINC 664 CTF Challenge](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [DCNextGen - Bricks in the Air](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Bricks in the Air](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [DCNextGen - RIC-1: ELT Localization Exercise - N3VR-G0N Down](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [DCNextGen - Space Grand Challenge - SatHack: The MOUSE-1 Mission](#) -
[AI Village](#) - cont...(10:00-17:59 PDT) - [AI Village: Village Open](#) -
[AI Village](#) - cont...(10:00-17:59 PDT) - [Cyber Mirage: Realtime Deepfake Demos](#) - Brandon Kovacs
[AI Village](#) - cont...(10:00-17:59 PDT) - [Poster Presentations](#) -
[AI Village](#) - [MeshLens: Security Profiling at Scale](#) - Vipul Ujawane,Jigar Bhavsar,Rayden Chia
[AI Village](#) - (16:30-16:59 PDT) - [Trust Amplification in Enterprise AI Systems – Microsoft CoPilot Case Studies Enabling AI-Assisted Influence Operations](#) - Tobias Diehl
[AppSec Village](#) - cont...(15:15-16:15 PDT) - [Proactive Malicious Package Defense](#) - Darren Meyer
[AppSec Village](#) - (16:30-17:30 PDT) - [Your SaaS Is My Foothold: Weaponizing Shadow SaaS for Initial Access and Persistence](#) - Jordan Bonagura
[AppSec Village](#) - (16:15-17:59 PDT) - [Code to Cloud: Secure Modern Applications Using Open-Source Tools](#) - Mackenzie
[AppSec Village](#) - [The API Made Me Do It - Do Bad APIs Lead AI to Generate Vulnerable Code?](#) - Yariv Tal
[AppSec Village](#) - (16:50-17:20 PDT) - [No Jailbreak Required: Pwning AI Agents Through the Tools They Trust](#) - Helen Oakley,saikishu
[AppSec Village](#) - cont...(15:00-16:59 PDT) - [SBOM Find the Flaws](#) - Dmitry Raidman
[AppSec Village](#) - cont...(15:00-16:59 PDT) - [AppSec Quiz Gauntlet: Spot the Vulnerability](#) - Avek Kolech
[AppSec Village](#) - cont...(15:00-16:59 PDT) - [AI Pentesting Trivia Showdown](#) - Andy Dennis,William Reyor
[AppSec Village](#) - cont...(15:00-16:59 PDT) - [The Call Stack Experience](#) - Victoria Keeler
[Biohacking Village](#) - cont...(10:00-17:59 PDT) - [Biohacking Device Lab](#) -
[Biohacking Village](#) - cont...(10:00-17:59 PDT) - [Embedded & Shredded: Advanced Embedded System Hacking](#) -
[Blacks In Cyber Village](#) - [Improving Security Vulnerability Descriptions using LLMs](#) - Kenechukwu Nwodo
[Blacks In Cyber Village](#) - (16:30-16:59 PDT) - [\[Virtual\] National Service Panel - CTU,BIC,MCPA](#) - Carmeshia Miller,Tiffany Scheurenbrand,Shemeka Chance Jeffrey
[Blue Team Village](#) - cont...(15:45-16:45 PDT) - [Threat Hunting Explained Badly](#) - Alllison Gallo,Brian Baskin,Silas Cutler,Sydney "letswastetime" Marrone
[Bug Bounty Village](#) - [Burp, But Yours: Hands-On Extension and Bambda Development](#) - Hannah L
[Call Center Village](#) - cont...(10:00-17:59 PDT) - [Call Center Village - Open](#) -
[Car Hacking Village](#) - cont...(10:00-16:59 PDT) - [Bomb Bot Challenge](#) -
[Car Hacking Village](#) - cont...(10:00-17:59 PDT) - [Car Hacking Village Open](#) -
[Car Hacking Village](#) - [Free IP, Free Chaos: DHCP-Assisted Flooding Against Automotive Ethernet](#) - Yehyeong Lee
[Cloud Village](#) - [OCIguana - A vulnerable-by-design OCI lab](#) - Eli Shparaga
[Cloud Village](#) - [Securing the AI Stack and Hunting Across Clouds](#) - Bryant Pickford
[Cloud Village](#) - [The 100-to-1 Problem: Securing the Non-Human Identity Perimeter](#) -
[Cloud Village](#) - (16:40-17:20 PDT) - [Key Rotation Won't Save You: Hunting Workload Identity Backdoors in AWS and GCP](#) - Jie Wu

[CodeBloom - What is AI? - Sam Mosley](#)
[Contests - cont...\(10:00-17:59 PDT\) - 5N4CK3Y -](#)
[Contests - cont...\(10:00-17:59 PDT\) - DC's Next Top Threat Model -](#)
[Contests - cont...\(10:00-17:59 PDT\) - Untechnical -](#)
[Contests - cont...\(10:00-17:59 PDT\) - DEF CON Scavenger Hunt -](#)
[Contests - cont...\(10:00-17:59 PDT\) - Darknet-NG -](#)
[Contests - cont...\(10:00-17:59 PDT\) - Crack Me If You Can 2026 -](#)
[Contests - cont...\(10:00-17:59 PDT\) - TeleChallenge -](#)
[Contests - cont...\(10:00-17:59 PDT\) - HackFortress -](#)
[Contests - cont...\(10:00-17:59 PDT\) - ?Cube -](#)
[Contests - cont...\(10:00-17:59 PDT\) - \\$unLight Sh4d0w5 -](#)
[Contests - cont...\(10:00-17:59 PDT\) - Octopus Game - Booth Open -](#)
[Contests - cont...\(10:00-17:59 PDT\) - Beer Chilling Contraption Contest -](#)
[Contests - cont...\(10:00-17:59 PDT\) - Cryptid Hunt -](#)
[Contests - cont...\(10:00-17:59 PDT\) - HSPACE: AI Battlegrounds -](#)
[Contests - cont...\(10:00-17:59 PDT\) - spyVspy 3: Rat Race -](#)
[Contests - cont...\(10:00-17:59 PDT\) - Hacker Games -](#)
[Contests - cont...\(10:00-17:59 PDT\) - PhreakMe -](#)
[Contests - cont...\(10:00-17:59 PDT\) - Game Hacking Village CTF -](#)
[Contests - cont...\(10:00-17:59 PDT\) - Kubernetes CTF -](#)
[Contests - cont...\(10:00-17:59 PDT\) - Hac-Man -](#)
[Contests - cont...\(10:00-17:59 PDT\) - Crack the Core -](#)
[Contests - cont...\(10:00-17:59 PDT\) - Cyber Deck Competition -](#)
[Contests - cont...\(10:00-17:59 PDT\) - Pinball High Score Contest -](#)
[Contests - cont...\(10:00-17:59 PDT\) - Code Cadaver: Break Every System. Save Your Friend. -](#)
[Contests - cont...\(10:00-17:59 PDT\) - PWN UR H0M3 - DDoS CTF -](#)
[Contests - cont...\(10:00-17:59 PDT\) - Real7y Overrun - Contest running -](#)
[Contests - cont...\(10:00-17:59 PDT\) - Tin Foil Hat Contest -](#)
[Contests - cont...\(10:00-17:59 PDT\) - CMD+CTRL Cyber Range: DarkMoney -](#)
[Contests - cont...\(15:30-17:30 PDT\) - Locktopus Challenge Finals -](#)
[Contests - cont...\(10:00-17:59 PDT\) - Radio Frequency Capture the Flag -](#)
[Contests - cont...\(10:00-17:59 PDT\) - DEF CON CTF: Benevolent Bureau of Birds -](#)
[Contests - cont...\(10:00-17:59 PDT\) - AI Village Plays Pokemon: DEFCON Edition - Nick Ashworth](#)
[Contests - cont...\(10:00-17:59 PDT\) - AI Village - Hal CTF -](#)
[Contests - cont...\(10:00-16:59 PDT\) - Car Hacking Village CTF -](#)
[Contests - cont...\(10:00-17:59 PDT\) - OWASP CTF -](#)
[Contests - cont...\(10:00-17:59 PDT\) - Escalation Desk CTF -](#)
[Contests - cont...\(10:00-17:59 PDT\) - DEF CON Groups Backdoors & Breaches - Tim Doerges,Seth Benning](#)
[Contests - cont...\(10:00-17:59 PDT\) - DEF CON Groups Sticker Contest -](#)
[Contests - cont...\(10:00-23:59 PDT\) - Apex Park \(Cloud Village CTF\) -](#)
[Contests - cont...\(10:00-17:59 PDT\) - Hacking GRC Contest -](#)
[Crypto & Privacy Village - Quantum-Ready or Not: What 1,000 Codebases Reveal About Cryptographic Risk - Dr. Zulfikar Ramzan](#)
[Cryptocurrency Village - Breaking Ciphers and Zero-Knowledge Proofs - Luke Szramowski,Freeman Slaughter,Diego "rehrrar" Salazar](#)
[Data Duplication Village - cont...\(10:00-17:59 PDT\) - DDV open and accepting drives for duplication -](#)
[DCNextGen - 3D Printing: Data, Discretion, and Design - Evan](#)
[DEF CON Groups - cont...\(10:00-17:59 PDT\) - DEF CON Groups \(DCG\) -](#)
[DEF CON Talks - Hacking Your Life with AI Can Get You Hacked: How AI Orchestration Platforms Ship RCE by Design - Peyton "p80n-sec" Kennedy](#)
[DEF CON Talks - cont...\(15:30-16:30 PDT\) - Zero-Day Provisioning: Chaining TP-Link ZTP Vulnerabilities for Infiltrating Networks - Francesco La Spina,Stanislav Dashevskiy](#)
[DEF CON Talks - \(16:30-17:30 PDT\) - How much of our Bluetooth firmware reverse engineering work can now be automated with LLMs? - Veronica Kovah,Xeno Kovah](#)
[DEF CON Talks - The Compiler That Can't Read: Crashing Every 5G Phone With One Byte - Qiqing Huang,Xingyu Wang](#)

DEF CON Talks - cont...(15:30-16:30 PDT) - [Wrestling with a Python: Escaping Copilot Studio's AI-Guarded Sandbox](#) - Ryan Hausknecht, Simon Maxwell-Stewart

DEF CON Talks - (16:30-17:30 PDT) - [Taming the Swarm: Hard Architectural Lessons from Building a Deterministic Agentic Web Pentesting System](#) - Albert "yz9yt" Corzo

DEF CON Talks - [Install Me Maybe: Turning Claimable VS Code Extension IDs into Supply-Chain Attacks](#) - Raphael "rcss" Silva

DEF CON Training - cont...(08:30-17:30 PDT) - [Blue vs Red Bootcamp: From Attacker Playbooks to Defender Detections](#) - Carlo Anez Mazurco, Mariana Ruiz

DEF CON Training - cont...(08:30-17:30 PDT) - [Influence Operations: Tactics, Defense, and Exploitation](#) - Greg Conti, Tom Cross

DEF CON Training - cont...(08:30-17:30 PDT) - [Full-Stack Pentesting Laboratory: 100% Hands-On + Lifetime LAB Access](#) - Dawid Czagan

DEF CON Workshops - cont...(14:00-17:59 PDT) - [Sold Out - Hands-on DuckyScript: An Introduction to HID Attack Tools with O.MG Devices](#) - wasabi, Ø1, Tokugero

DEF CON Workshops - cont...(14:00-17:59 PDT) - [Sold Out - Purple Teaming Industrial Control Systems](#) - Arnaud SOULLIE, Alexandrine Torrents

DEF CON Workshops - cont...(14:00-17:59 PDT) - [Sold Out - Entra ID Persistence - Because Passwords Were Never the Problem](#) - Raunak "Trouble1" Parmar, Chirag "3xpl01tc0d3r" Savla

DEF CON Workshops - cont...(14:00-17:59 PDT) - [Sold Out - From Prompt to PWN: Exploiting LLM Powered Web Applications with OWASP Techniques](#) - Abhinav Verma

DEF CON Workshops - cont...(14:00-17:59 PDT) - [Sold Out - Intro to Writing Windows Malware with Rust!](#) - iDigitalFlame, Daniel Bravo

DEF CON Workshops - cont...(14:00-17:59 PDT) - [Sold Out - Building Agentic Reverse Engineering "Skills"](#) - John "clearbluejar" McIntosh

DEF CON Workshops - cont...(14:00-17:59 PDT) - [Sold Out - Learning to Reverse Engineer Compiled C as We Learn to Write It](#) - Wesley McGrew

DEF CON Workshops - cont...(14:00-17:59 PDT) - [Sold Out - Salesforce Apex Predator: Breaking Salesforce Sites](#) - Nitay Bachrach, Cynthia Ardman

Demo Labs - [xEndity: IoT Firmware Analysis & Digital Twin Platform](#) - Zeus "LightningGod" Chan, Kenneth "kenleejl" Lee

Demo Labs - [GnawLab: Open-Source AWS Attack Scenarios Based on Real-World Breaches](#) - ialleejy, Kyul, HyunJun "Beaver King" Kwon

Demo Labs - [VoiceLock: Offline, Robust On-Device Speech Transcription](#) - Ayaan Qayyum, Parag Kalay

Demo Labs - [Zero-Cloud Threat Modeling: Vector Embedding Architectures for Automated Vulnerability Detection](#) - Ankit Vashisth

Demo Labs - [Weaponizing eBPF and XDP with Covert Triggered Reverse Shells](#) - Yll "0xBabar0ka" Berisha

Demo Labs - [Overcast: Video OSINT Agent. Point It at 100 Videos, Ask Anything](#) - Kevin "kdrwins" Dela Rosa

Embedded Systems Village - cont...(10:00-17:59 PDT) - [Exploit Bluetooth Low Energy with BLESPlloit and optional ESP32](#) - Slawomir Jasek

Embedded Systems Village - cont...(10:00-17:59 PDT) - [Thread Carefully](#) -

Embedded Systems Village - cont...(10:00-17:59 PDT) - [Embedded - 101 Labs](#) -

Embedded Systems Village - cont...(10:00-17:59 PDT) - [Embedded Systems Village CTF](#) -

Game Hacking Village - cont...(10:00-16:59 PDT) - [Riot Games Vanguard: Pwn to own](#) -

Game Hacking Village - [Chill Zone: Smash \(Project Plus\) Tournament with Prizes](#) -

Game Hacking Village - [Dreamcast Ex Inferis — RCE on the Sega Dreamcast PlanetWeb Internet Browser v3.0](#) - Piffd0s

Ham Radio Village - [Keeping the Angry Pixies Happy: the Care and Feeding of your Batteries](#) - hamster

IoT Village - cont...(10:00-17:59 PDT) - [Smart Home in the Matter: Blink, Race, Attack CTF](#) -

IoT Village - cont...(10:00-17:59 PDT) - [Expose Hidden Surveillance in Everyday Tech](#) -

IoT Village - cont...(10:00-17:59 PDT) - [Discover GE Appliances!](#) -

IoT Village - cont...(10:00-17:59 PDT) - [All About UART](#) -

IoT Village - cont...(10:00-17:59 PDT) - [Raiders of the Lost Firmware: A Hands-On Workshop in IoT Firmware Archaeology](#) -

IoT Village - cont...(10:00-17:59 PDT) - [Hands-On Hardware Hacking – From JTAG to Root, Memory Patching Boot Process for Root Access](#) -

IoT Village - cont...(10:00-17:59 PDT) - [Just Hacking Training](#) -

IoT Village - cont...(10:00-17:59 PDT) - [Cat-astrophic Hacking: Breaking Into Smart Litter Boxes](#) -

IoT Village - cont...(15:00-16:30 PDT) - [Mesh Nets for Hackers: How \(& When\) to use Meshtastic, Meshcore, & Reticulum!](#) - Kody Kinzie

IoT Village - (16:30-17:30 PDT) - [Weaponization of Cellular Based IoT Technology – Leveraging Smart Devices to Gain a Foothold](#) - Carlota Bindner,Deral Heiland

La Villa Community - cont...(15:30-16:30 PDT) - [From Live Malware to Red Team Tradecraft: Process Hollowing in msbuild.exe](#) - Filipi Pires

La Villa Community - (16:30-17:30 PDT) - [De la Explotación de Buffer Overflows al C2 Industrial: Infectando y Controlando RTUs con Malware](#) - Fernando Mengali

Lonely Hackers Club - cont...(10:00-17:59 PDT) - [Lonely Hackers Club CTF](#) -

Lonely Hackers Club - cont...(10:00-17:59 PDT) - [Lonely Hackers Club - Sticker Swap Table](#) -

Lonely Hackers Club - cont...(10:00-17:59 PDT) - [Lonely Hackers Club - Lockpicking Table](#) -

Lonely Hackers Club - cont...(10:30-16:30 PDT) - [Resume Review with the Lonely Hackers Club](#) -

Maker's Village - cont...(10:00-17:59 PDT) - [Makers' Village - Hacker Arts and Crafts](#) -

Maker's Village - cont...(15:00-16:59 PDT) - [Cyberdeck Build](#) - Sk!tz0

Maker's Village - [Building Silkscreens and carving stamps](#) - hunny

Malware Village - cont...(15:20-16:05 PDT) - [Leigh Trinity OTW](#) - Leigh Gilbert

Malware Village - (16:15-16:55 PDT) - [The AI Analysis Train is Leaving the Station: ALL ABOARD!!](#) - Ryan "@rj_chap" Chapman

Malware Village - cont...(14:10-16:50 PDT) - [An Intro to Mac Malware Analysis](#) - Patrick Wardle

Maritime Hacking Village - [Shipcrawler: Automated Maritime OSINT — From Open Data to Actionable Intelligence](#) - Ahmed Nagi Nasr

Maritime Hacking Village - (16:30-16:59 PDT) - [LSTM Autoencoder Ensemble for NMEA 2000 Intrusion Detection on Vessel Networks](#) - Anissa Elias,James Campbell

Misc - cont...(15:30-16:30 PDT) - [Privacy's Defender with Women in Security and Privacy \(WISP\)](#) - Cindy Cohn,Alyssa Coley

Mobile Hacking Community - cont...(10:00-17:59 PDT) - [Mobile Hacking - Informal CTF](#) -

Mobile Hacking Community - cont...(10:00-17:59 PDT) - [Mobile Hacking Community - Open](#) -

Nix Vegas Community - cont...(15:30-16:30 PDT) - [Your Infrastructure Is a DAG: Manage It With Nix](#) - Ethan Carter Edwards

Nix Vegas Community - (16:30-16:59 PDT) - [Breaking the Chains of Cloud Giants: Building a Fully Autonomous Personal Cloud on NixOS](#) - Maksim Kuskov,Mikhail Ilin

Noob Community - cont...(10:00-17:59 PDT) - [No Stupid Questions](#) -

Noob Community - cont...(10:00-17:59 PDT) - [TCM Security Labs](#) -

Noob Community - cont...(10:00-17:59 PDT) - [Skillbit Labs](#) -

Noob Community - cont...(10:00-17:59 PDT) - [SANS Institute NetWars Labs](#) -

Noob Community - cont...(10:00-17:59 PDT) - [Hack The Box DC Junior Ranger Program Challenge](#) -

Noob Community - cont...(10:00-17:59 PDT) - [Kryptsec Labs](#) -

Noob Community - cont...(10:00-17:59 PDT) - [Arcanum Security Labs](#) -

Noob Community - cont...(10:00-17:59 PDT) - [Mentoring and Career Advice](#) -

Noob Community - cont...(15:00-16:59 PDT) - [AI Hacking for Noobs](#) - Jason "jhaddix" Haddix,Arcanum Information Security Team

Noob Community - (16:15-16:45 PDT) - [Imposter Syndrome Is Distracting You From the Work That Matters](#) - Samantha Schwartz

OSINT For Good Community - cont...(10:00-17:59 PDT) - [FINDX OSINT Educational Series](#) -

OSINT For Good Community - cont...(10:00-17:59 PDT) - [OSINT4Good Community - DC NextGen Content](#) -

OSINT For Good Community - [OSINT Search party CTF Debrief](#) - Trace Labs Staff

OWASP Foundation - cont...(10:00-17:59 PDT) - [BadVR: Signals Everywhere a collaboration with XR Village](#) - Jad Meouchy,Suzanne Borders

OWASP Foundation - [Practical AI Security Assessments Using OWASP AISVS](#) - Jim Manico

Packet Hacking Village - [Why Couldn't I See My Own Drone? Remote ID, ESP32s, and the Packet Trail to Friend or Foe](#) - Will Hatzer,Charles Grow

Payment Village - [Compounding Interest: Exploiting the ATM Supply Chain](#) - Matt Burch

Physical Security Village - [Zero-Knowledge Unsaflok: The Unsaflok Saga Continues](#) - Ben Higgins,Aaron Tulino

Policy @ DEF CON - [Securing the Safety Net: Why Healthcare Cybersecurity Policy Keeps Failing Patients](#) - Sahan Fernando,James Bowie,Nancy Brainerd,Phil Englert

Radio Frequency Village - cont...(10:00-17:59 PDT) - Radio Frequency Village Events -
Radio Frequency Village - Yes, it runs Doom: over the air gaming on a bladeRF SDR - max
Radio Frequency Village - (16:30-17:25 PDT) - I'm Not Special, and You Can Too! A journey into RF Antenna Design for Dummies. - Hamspiced
Recon Village - cont...(11:00-16:59 PDT) - GE(O)SINT Contest -
Recon Village - cont...(12:00-17:59 PDT) - TrackTheFugitive Contest -
Recon Village - cont...(15:20-17:50 PDT) - Vibe Coding Your Way to a Fully Functional Open-Source Intelligence Platform - Lenin Alevski
Recon Village - Live Recon Contest — Final Presentations -
Red Team Village - The Quantum Mechanic: Attacking all the clouds - Moses Frost
Red Team Village - Evading EDR in ATM - Arnold Jared Morales Yopez
Red Team Village - MalSkill: Weaponizing AI Agent Skills for Persistence, Exfiltration, and Lateral Movement - Nur Gucu
Red Team Village - Writing Production-Grade Exploits in go-exploit - Landon Rice
Red Team Village - Control + C = Control Me - Andrew Griess
Red Team Village - OSINT for Hackers Redux - Lee McWhorter,Sandra Stibbards
Scambait Village - cont...(10:00-17:59 PDT) - Open Q&A -
Scambait Village - cont...(10:00-17:59 PDT) - KSCM Scambait Radio -
Scambait Village - cont...(15:30-16:59 PDT) - Creator Drop-In -
Social Engineering Community Village - cont...(10:00-17:59 PDT) - Social Engineering Community Village - Open Hours -
Social Engineering Community Village - Wolfmasking: Teaching Everyday Defenders to Think Like Social Engineers - Brian Brushwood
Social Engineering Community Village - (16:30-17:59 PDT) - Cold Calls -
Social Engineering Community Village - cont...(15:30-17:30 PDT) - 2027 SECVC Pre-Qualification Round - JC,Snow
Social Gatherings/Events - cont...(09:00-18:59 PDT) - Human Registration Open -
Social Gatherings/Events - Book Signing - Thomas Wilhelm - Thomas Wilhelm
Social Gatherings/Events - Book Signing - Avinash Majeti - Avinash Majeti
Social Gatherings/Events - cont...(10:00-18:59 PDT) - Music - SomaFM -
Social Gatherings/Events - cont...(11:00-16:59 PDT) - Free Ham Radio License Exams -
Social Gatherings/Events - Queercon Mixer -
Social Gatherings/Events - cont...(15:00-16:59 PDT) - DCG New England Meetup -
Telecom Village - cont...(15:45-16:45 PDT) - Industry Challenges & SOC Reality - Vinod Shrimali
Telecom Village - (16:45-16:59 PDT) - Telecom Village CTF Closure -
The Diana Initiative - The Diana Initiative - Open time -
Voting Village - cont...(10:00-17:59 PDT) - Voting Village Lab -
Voting Village - Low Skill, High Impact Attacks on Internet Voting - John Odum
Voting Village - (16:30-16:59 PDT) - On the Weaponization of Voting Channels - Carsten Schürmann

[Return to Index](#) - [Locations Legend](#)

[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Flight Simulator/EFB](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [MOUSE Runner & Flappy Drone](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Drone Hacking Workshop](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Mission: Compromised - Hacking a Satellite from the Ground Up](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Drone Hacking Choose your Own Adventure](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Nebula Showdown: Space Systems Security CTF Adventure](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [SpaceCOP - Catch Me If You Can](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Satellites Under Attack: Hands-On Satellite Security Threat Scenarios](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [SR-71 Blackbird Badge Challenge](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [ARINC 664 CTF Challenge](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Aerospace Ecosystem Resilience Innovation Environment \(AERIE\) Cyber Range](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Aviation ISAC Cybersecurity Challenge](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [DCNextGen - RIC-1: ELT Localization Exercise - N3VR-G0N Down](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [DCNextGen - Bricks in the Air](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [Bricks in the Air](#) -
[Aerospace Village](#) - cont...(10:00-17:59 PDT) - [DCNextGen - Space Grand Challenge - SatHack: The MOUSE-1 Mission](#) -
[Aerospace Village](#) - [Behind the Badge: SAOV3 and Open Sourcing the Aerospace Village ISS Badge](#) - Adam Batori, Kevin Colley, Robert Pafford, Lillian Ash Baker
[Aerospace Village](#) - (17:30-17:59 PDT) - [SpaceCOP: Houston, We Have an Intrusion](#) - Brandon Bailey
[AI Village](#) - cont...(10:00-17:59 PDT) - [Cyber Mirage: Realtime Deepfake Demos](#) - Brandon Kovacs
[AI Village](#) - cont...(10:00-17:59 PDT) - [Poster Presentations](#) -
[AI Village](#) - cont...(10:00-17:59 PDT) - [AI Village: Village Open](#) -
[AI Village](#) - (17:30-17:59 PDT) - [SADF: A Taxonomy and Evaluation Framework for Agentic Security Failures](#) - Julie Brunias
[AppSec Village](#) - cont...(16:30-17:30 PDT) - [Your SaaS Is My Foothold: Weaponizing Shadow SaaS for Initial Access and Persistence](#) - Jordan Bonagura
[AppSec Village](#) - cont...(16:15-17:59 PDT) - [Code to Cloud: Secure Modern Applications Using Open-Source Tools](#) - Mackenzie
[AppSec Village](#) - cont...(16:50-17:20 PDT) - [No Jailbreak Required: Pwning AI Agents Through the Tools They Trust](#) - Helen Oakley, saikishu
[AppSec Village](#) - (17:30-17:59 PDT) - [From Prompts to Production: Discovering Exposed PII & IDORs in AI-Generated Apps](#) - Samantha Pearlstein
[Biohacking Village](#) - cont...(10:00-17:59 PDT) - [Biohacking Device Lab](#) -
[Biohacking Village](#) - cont...(10:00-17:59 PDT) - [Embedded & Shredded: Advanced Embedded System Hacking](#) -
[Blue Team Village](#) - [Incident Response in 2026](#) - Chriss Hansen, K Singh, Levone Campbell, Sarthak Taneja
[Bug Bounty Village](#) - cont...(16:00-17:59 PDT) - [Burp, But Yours: Hands-On Extension and Bambda Development](#) - Hannah L
[Call Center Village](#) - cont...(10:00-17:59 PDT) - [Call Center Village - Open](#) -
[Car Hacking Village](#) - cont...(10:00-17:59 PDT) - [Car Hacking Village Open](#) -
[Cloud Village](#) - cont...(16:00-17:59 PDT) - [OCIguana - A vulnerable-by-design OCI lab](#) - Eli Shparaga
[Cloud Village](#) - cont...(16:40-17:20 PDT) - [Key Rotation Won't Save You: Hunting Workload Identity Backdoors in AWS and GCP](#) - Jie Wu
[CodeBloom](#) - [Work Session: Binary Code](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [5N4CK3Y](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [DC's Next Top Threat Model](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Untechnical](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [DEF CON Scavenger Hunt](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Darknet-NG](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Crack Me If You Can 2026](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [TeleChallenge](#) -

[Contests](#) - cont...(10:00-17:59 PDT) - [HackFortress](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [?Cube](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [\\$unLight Sh4d0w5](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Octopus Game - Booth Open](#) -
[Contests](#) - [Octopus Game - The Final Booth Battle](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Beer Chilling Contraption Contest](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Cryptid Hunt](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [HSPACE: AI Battlegrounds](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [spyVspy 3: Rat Race](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Hacker Games](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [PhreakMe](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Game Hacking Village CTF](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Kubernetes CTF](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Hac-Man](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Crack the Core](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Cyber Deck Competition](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Pinball High Score Contest](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Code Cadaver: Break Every System. Save Your Friend.](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [PWN UR H0M3 - DDoS CTF](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Real7y Overrun - Contest running](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Tin Foil Hat Contest](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [CMD+CTRL Cyber Range: DarkMoney](#) -
[Contests](#) - cont...(15:30-17:30 PDT) - [Locktopus Challenge Finals](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Radio Frequency Capture the Flag](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [DEF CON CTF: Benevolent Bureau of Birds](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [AI Village - Hal CTF](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [AI Village Plays Pokemon: DEFCON Edition](#) - Nick Ashworth
[Contests](#) - cont...(10:00-17:59 PDT) - [OWASP CTF](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Escalation Desk CTF](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [DEF CON Groups Backdoors & Breaches](#) - Tim Doerges,Seth Benning
[Contests](#) - cont...(10:00-17:59 PDT) - [DEF CON Groups Sticker Contest](#) -
[Contests](#) - cont...(10:00-23:59 PDT) - [Apex Park \(Cloud Village CTF\)](#) -
[Contests](#) - cont...(10:00-17:59 PDT) - [Hacking GRC Contest](#) -
[Crypto & Privacy Village](#) - [The National Fight Against ALPRs](#) - Freddy Martinez,Sarah
[Data Duplication Village](#) - cont...(10:00-17:59 PDT) - [DDV open and accepting drives for duplication](#) -
[DCNextGen](#) - [Objectively Awesome Robots: A Hands-On Introduction to Python Classes and Objects](#) - 4ng3lhacker
[DEF CON Groups](#) - cont...(10:00-17:59 PDT) - [DEF CON Groups \(DCG\)](#) -
[DEF CON Talks](#) - [High Voltage Heist: Turning Your EV into my Power Bank](#) - Fabien Guillebot,Stepan Konicek
[DEF CON Talks](#) - cont...(16:30-17:30 PDT) - [How much of our Bluetooth firmware reverse engineering work can now be automated with LLMs?](#) - Veronica Kovah,Xeno Kovah
[DEF CON Talks](#) - (17:30-17:59 PDT) - [TEE.fail: Breaking Trusted Execution Environments via DDR5 Memory Bus Interposition](#) - Daniel Genkin,Jalen Chuang
[DEF CON Talks](#) - [OffGuard: Breaking the Most Popular AI Gateway from Auth Bypass to Cloud Compromise](#) - Yaara Shriki
[DEF CON Talks](#) - cont...(16:30-17:30 PDT) - [Taming the Swarm: Hard Architectural Lessons from Building a Deterministic Agentic Web Pentesting System](#) - Albert "yz9yt" Corzo
[DEF CON Talks](#) - (17:30-20:30 PDT) - [DEF CON Franklin: What worked, what didn't, and how we are giving agency to water utilities at the top of every bad guy's target list because of data centers](#) - Jake Braun
[DEF CON Talks](#) - [CRLF-Powered Desync Attacks: Beheading HTTP streams](#) - Tom "t0xodile" Stacey,Tobia "mastersplinter" Righi
[DEF CON Training](#) - cont...(08:30-17:30 PDT) - [Blue vs Red Bootcamp: From Attacker Playbooks to Defender Detections](#) - Carlo Anez Mazurco,Mariana Ruiz
[DEF CON Training](#) - cont...(08:30-17:30 PDT) - [Influence Operations: Tactics, Defense, and Exploitation](#) - Greg Conti,Tom Cross
[DEF CON Training](#) - cont...(08:30-17:30 PDT) - [Full-Stack Pentesting Laboratory: 100% Hands-On + Lifetime LAB Access](#) - Dawid Czagan

DEF CON Workshops - cont...(14:00-17:59 PDT) - Sold Out - Hands-on DuckyScript: An Introduction to HID Attack Tools with O.MG Devices - wasabi,Ø1,Tokugero

DEF CON Workshops - cont...(14:00-17:59 PDT) - Sold Out - Purple Teaming Industrial Control Systems - Arnaud SOULLIE,Alexandrine Torrents

DEF CON Workshops - cont...(14:00-17:59 PDT) - Sold Out - Entra ID Persistence - Because Passwords Were Never the Problem - Raunak "Trouble1" Parmar,Chirag "3xpl01tc0d3r" Savla

DEF CON Workshops - cont...(14:00-17:59 PDT) - Sold Out - From Prompt to PWN: Exploiting LLM Powered Web Applications with OWASP Techniques - Abhinav Verma

DEF CON Workshops - cont...(14:00-17:59 PDT) - Sold Out - Intro to Writing Windows Malware with Rust! - iDigitalFlame,Daniel Bravo

DEF CON Workshops - cont...(14:00-17:59 PDT) - Sold Out - Building Agentic Reverse Engineering "Skills" - John "clearbluejar" McIntosh

DEF CON Workshops - cont...(14:00-17:59 PDT) - Sold Out - Learning to Reverse Engineer Compiled C as We Learn to Write It - Wesley McGrew

DEF CON Workshops - cont...(14:00-17:59 PDT) - Sold Out - Salesforce Apex Predator: Breaking Salesforce Sites - Nitay Bachrach,Cynthia Ardman

Embedded Systems Village - cont...(10:00-17:59 PDT) - Embedded - 101 Labs -

Embedded Systems Village - cont...(10:00-17:59 PDT) - Thread Carefully -

Embedded Systems Village - cont...(10:00-17:59 PDT) - Exploit Bluetooth Low Energy with BLESPlloit and optional ESP32 - Slawomir Jasek

Embedded Systems Village - cont...(10:00-17:59 PDT) - Embedded Systems Village CTF -

IoT Village - cont...(10:00-17:59 PDT) - All About UART -

IoT Village - cont...(10:00-17:59 PDT) - Expose Hidden Surveillance in Everyday Tech -

IoT Village - cont...(10:00-17:59 PDT) - Smart Home in the Matter: Blink, Race, Attack CTF -

IoT Village - cont...(10:00-17:59 PDT) - Discover GE Appliances! -

IoT Village - cont...(10:00-17:59 PDT) - Raiders of the Lost Firmware: A Hands-On Workshop in IoT Firmware Archaeology -

IoT Village - cont...(10:00-17:59 PDT) - Hands-On Hardware Hacking – From JTAG to Root, Memory Patching Boot Process for Root Access -

IoT Village - cont...(10:00-17:59 PDT) - Just Hacking Training -

IoT Village - cont...(10:00-17:59 PDT) - Cat-astrophic Hacking: Breaking Into Smart Litter Boxes -

IoT Village - cont...(16:30-17:30 PDT) - Weaponization of Cellular Based IoT Technology – Leveraging Smart Devices to Gain a Foothold - Carlota Bindner,Deral Heiland

La Villa Community - cont...(16:30-17:30 PDT) - De la Explotación de Buffer Overflows al C2 Industrial: Infectando y Controlando RTUs con Malware - Fernando Mengali

La Villa Community - (17:30-18:30 PDT) - latinax.exe has entered the chat (ESP - POR) -

Lonely Hackers Club - cont...(10:00-17:59 PDT) - Lonely Hackers Club - Sticker Swap Table -

Lonely Hackers Club - cont...(10:00-17:59 PDT) - Lonely Hackers Club - Lockpicking Table -

Lonely Hackers Club - cont...(10:00-17:59 PDT) - Lonely Hackers Club CTF -

Maker's Village - cont...(10:00-17:59 PDT) - Makers' Village - Hacker Arts and Crafts -

Maker's Village - cont...(16:00-17:45 PDT) - Building Silkscreens and carving stamps - hunny

Middle Easterns & Africans in Cyber Security (MEACS) - (17:30-17:59 PDT) - The Autonomous SOC Blueprint: On-Premise ML & AI to Condense, Consolidate, Contextualize, Correlate & Co-Investigate Attack Chains Hiding in the Noise - Ezz Tahoun

Middle Easterns & Africans in Cyber Security (MEACS) - MEACS Trivia, Games and Networking -

Mobile Hacking Community - cont...(10:00-17:59 PDT) - Mobile Hacking Community - Open -

Mobile Hacking Community - cont...(10:00-17:59 PDT) - Mobile Hacking - Informal CTF -

Nix Vegas Community - Lightning Talks and Unconference -

Noob Community - cont...(10:00-17:59 PDT) - TCM Security Labs -

Noob Community - cont...(10:00-17:59 PDT) - Skillbit Labs -

Noob Community - cont...(10:00-17:59 PDT) - SANS Institute NetWars Labs -

Noob Community - cont...(10:00-17:59 PDT) - No Stupid Questions -

Noob Community - cont...(10:00-17:59 PDT) - Mentoring and Career Advice -

Noob Community - cont...(10:00-17:59 PDT) - Arcanum Security Labs -

Noob Community - cont...(10:00-17:59 PDT) - Kryptsec Labs -

Noob Community - cont...(10:00-17:59 PDT) - [Hack The Box DC Junior Ranger Program Challenge](#) -
 OSINT For Good Community - cont...(10:00-17:59 PDT) - [OSINT4Good Community - DC NextGen Content](#) -
 OSINT For Good Community - cont...(10:00-17:59 PDT) - [FINDX OSINT Educational Series](#) -
 OSINT For Good Community - [OSINT Search Party CTF Prize and Award Announcements](#). -
 OSINT For Good Community - (17:15-17:59 PDT) - [OSINT4Good Sticker Swap](#) -
 OWASP Foundation - cont...(10:00-17:59 PDT) - [BadVR: Signals Everywhere a collaboration with XR Village](#) - Jad Meouchy,Suzanne Borders
 OWASP Foundation - cont...(16:00-17:59 PDT) - [Practical AI Security Assessments Using OWASP AISVS](#) - Jim Manico
 Packet Hacking Village - [Ghost Followers: Using AI to Unmask Fake LinkedIn Profiles at Scale](#) - Aiswarya Venkitesh
 Policy @ DEF CON - [AI Safety Theater: What the RAISE Act Regulates — and What It Does Not](#) - Joshua Marpet
 Policy @ DEF CON - [The Closing Window: Governing Agentic AI Security in a Post-Mythos World](#) - Taylor Roberts,Mitch Herckis,Katie Trimble-Noble,Razvan Gavrila
 Radio Frequency Village - cont...(10:00-17:59 PDT) - [Radio Frequency Village Events](#) -
 Radio Frequency Village - cont...(16:30-17:25 PDT) - [I'm Not Special, and You Can Too! A journey into RF Antenna Design for Dummies](#). - Hamspiced
 Radio Frequency Village - (17:30-17:55 PDT) - [\\$750 and a Weekend: Passive Direction Finding Across the Spectrum with KrakenSDR](#) - K0YTL
 Recon Village - cont...(12:00-17:59 PDT) - [TrackTheFugitive Contest](#) -
 Recon Village - cont...(15:20-17:50 PDT) - [Vibe Coding Your Way to a Fully Functional Open-Source Intelligence Platform](#) - Lenin Alevski
 Recon Village - (17:30-17:59 PDT) - [Total Recon: How We Discovered 1000s of open Agents in The Wild](#) - Avishai Efrat,Roey Ben Chaim
 Recon Village - [CyberKB: When Your AI Copilot Runs the Recon, Crawls the Dark Web, and Maps the Kill Chain](#) - Suriya Prasath S,Chandru J,Muthu Kumar
 Recon Village - (17:30-17:59 PDT) - [There Is No Internet: Cross-Domain Recon of all 4.3 Billion IPv4s](#) - John McCary
 Red Team Village - cont...(16:00-17:59 PDT) - [The Quantum Mechanic: Attacking all the clouds](#) - Moses Frost
 Red Team Village - cont...(16:00-17:59 PDT) - [Evading EDR in ATM](#) - Arnold Jared Morales Yopez
 Red Team Village - cont...(16:00-17:59 PDT) - [MalSkill: Weaponizing AI Agent Skills for Persistence, Exfiltration, and Lateral Movement](#) - Nur Gucu
 Red Team Village - cont...(16:00-17:59 PDT) - [Writing Production-Grade Exploits in go-exploit](#) - Landon Rice
 Red Team Village - [Below the Threshold: Real-World APT Tradecraft for Full-Spectrum Compromise](#) - Jonathan Coradi,Oliveira Junior
 Scambait Village - cont...(10:00-17:59 PDT) - [Open Q&A](#) -
 Scambait Village - cont...(10:00-17:59 PDT) - [KSCM Scambait Radio](#) -
 Social Engineering Community Village - cont...(10:00-17:59 PDT) - [Social Engineering Community Village - Open Hours](#) -
 Social Engineering Community Village - cont...(16:30-17:59 PDT) - [Cold Calls](#) -
 Social Engineering Community Village - cont...(15:30-17:30 PDT) - [2027 SECVC Pre-Qualification Round](#) - JC,Snow
 Social Gatherings/Events - cont...(09:00-18:59 PDT) - [Human Registration Open](#) -
 Social Gatherings/Events - cont...(10:00-18:59 PDT) - [Music](#) - SomaFM -
 Social Gatherings/Events - [Friends of Bill W](#) -
 Social Gatherings/Events - cont...(16:00-17:59 PDT) - [Queercon Mixer](#) -
 Telecom Village - [Telecom Village Open Forum: Talks & Workshops: Review, Highlights, and Key Learnings](#) -
 The Diana Initiative - cont...(16:00-17:59 PDT) - [The Diana Initiative - Open time](#) -
 Voting Village - cont...(10:00-17:59 PDT) - [Voting Village Lab](#) -
 Voting Village - [Election Observation: Watching is not Enough](#) - Douglas W. Jones
 Voting Village - (17:30-17:59 PDT) - [The Republic is a Team Sport: Technology can Protect Elections, but the People must Protect Democracy](#) - Kendall Spencer

[Return to Index](#) - [Locations Legend](#)

[Contests](#) - [EFF Tech Trivia](#) -

[Contests](#) - [cont...\(10:00-23:59 PDT\)](#) - [Apex Park \(Cloud Village CTF\)](#) -

[DEF CON Talks](#) - [cont...\(17:30-20:30 PDT\)](#) - [DEF CON Franklin: What worked, what didn't, and how we are giving agency to water utilities at the top of every bad guy's target list because of data centers](#) - [Jake Braun](#)

[La Villa Community](#) - [cont...\(17:30-18:30 PDT\)](#) - [latinas.exe has entered the chat \(ESP - POR\)](#) -

[Social Gatherings/Events](#) - [cont...\(09:00-18:59 PDT\)](#) - [Human Registration Open](#) -

[Social Gatherings/Events](#) - [10 years of K-rad \(Hackers.Town Party\)](#) -

[Social Gatherings/Events](#) - [cont...\(10:00-18:59 PDT\)](#) - [Music](#) - [SomaFM](#) -

[Social Gatherings/Events](#) - [+61: the Australian Embassy](#) -

[Social Gatherings/Events](#) - [2nd Annual Spades Night & Uno Tournament](#) -

Saturday - 19:00 PDT

[Return to Index](#) - [Locations Legend](#)

[Contests](#) - cont...(18:00-20:59 PDT) - [EFF Tech Trivia](#) -

[Contests](#) - cont...(10:00-23:59 PDT) - [Apex Park \(Cloud Village CTF\)](#) -

[DEF CON Talks](#) - cont...(17:30-20:30 PDT) - [DEF CON Franklin: What worked, what didn't, and how we are giving agency to water utilities at the top of every bad guy's target list because of data centers](#) - [Jake Braun](#)

[Social Gatherings/Events](#) - cont...(18:00-20:59 PDT) - [10 years of K-rad \(Hackers.Town Party\)](#) -

[Social Gatherings/Events](#) - [Music](#) - [Genre: Dubstep](#) - [ZipZapZop](#)

[Social Gatherings/Events](#) - cont...(18:00-19:59 PDT) - [+61: the Australian Embassy](#) -

[Social Gatherings/Events](#) - [DCNextGen Party!](#) -

[Social Gatherings/Events](#) - cont...(18:00-22:59 PDT) - [2nd Annual Spades Night & Uno Tournament](#) -

Saturday - 20:00 PDT

[Return to Index](#) - [Locations Legend](#)

[Contests](#) - cont...(18:00-20:59 PDT) - [EFF Tech Trivia](#) -

[Contests](#) - cont...(10:00-23:59 PDT) - [Apex Park \(Cloud Village CTF\)](#) -

[DEF CON Talks](#) - cont...(17:30-20:30 PDT) - [DEF CON Franklin: What worked, what didn't, and how we are giving agency to water utilities at the top of every bad guy's target list because of data centers](#) - [Jake Braun](#)

[Social Gatherings/Events](#) - [Hacker Jeopardy](#) -

[Social Gatherings/Events](#) - cont...(18:00-20:59 PDT) - [10 years of K-rad \(Hackers.Town Party\)](#) -

[Social Gatherings/Events](#) - [Music - Genre: Drum & Bass](#) - [RELAY](#)

[Social Gatherings/Events](#) - [Movie Night](#) -

[Social Gatherings/Events](#) - [Hacker Karaoke](#) -

[Social Gatherings/Events](#) - cont...(19:00-20:59 PDT) - [DCNextGen Party!](#) -

[Social Gatherings/Events](#) - cont...(18:00-22:59 PDT) - [2nd Annual Spades Night & Uno Tournament](#) -

Saturday - 21:00 PDT

[Return to Index](#) - [Locations Legend](#)

[Contests](#) - [cont...\(10:00-23:59 PDT\)](#) - [Apex Park \(Cloud Village CTF\)](#) -
[Social Gatherings/Events](#) - [cont...\(20:00-21:59 PDT\)](#) - [Hacker Jeopardy](#) -
[Social Gatherings/Events](#) - [GOTHCON](#) -
[Social Gatherings/Events](#) - [Music](#) - [Genre: Nerdcore](#) - [Dual Core](#)
[Social Gatherings/Events](#) - [Front Man's Fête: An Octopus Game Party \(including Octopus Game winners and prizes\)](#) -
[Social Gatherings/Events](#) - [Party Line \(Call Center Village Party\)](#) -
[Social Gatherings/Events](#) - [cont...\(20:00-23:59 PDT\)](#) - [Movie Night](#) -
[Social Gatherings/Events](#) - [cont...\(18:00-22:59 PDT\)](#) - [2nd Annual Spades Night & Uno Tournament](#) -
[Social Gatherings/Events](#) - [VETCON 2026 PARTY](#) -
[Social Gatherings/Events](#) - [Illuminati Party](#) -

Saturday - 22:00 PDT

[Return to Index](#) - [Locations Legend](#)

[Contests](#) - [Feet Feud \(Hacker Family Feud\)](#) -

[Contests](#) - cont...(10:00-23:59 PDT) - [Apex Park \(Cloud Village CTF\)](#) -

[Social Gatherings/Events](#) - [Kayos Klub](#) -

[Social Gatherings/Events](#) - [Music](#) - [Genre: Drum & Bass](#) - [Miss Jackalope](#)

[Social Gatherings/Events](#) - cont...(20:00-23:59 PDT) - [Movie Night](#) -

[Social Gatherings/Events](#) - cont...(18:00-22:59 PDT) - [2nd Annual Spades Night & Uno Tournament](#) -

Saturday - 23:00 PDT

[Return to Index](#) - [Locations Legend](#)

[Contests](#) - cont...(22:00-23:59 PDT) - [Feet Feud \(Hacker Family Feud\)](#) -
[Contests](#) - cont...(10:00-23:59 PDT) - [Apex Park \(Cloud Village CTF\)](#) -
[Social Gatherings/Events](#) - [Music](#) - [Genre: Drum & Bass](#) - Syntax + Luna
[Social Gatherings/Events](#) - cont...(20:00-23:59 PDT) - [Movie Night](#) -

Sunday

This Schedule is tentative and may be changed at any time. Check [here](#), [Hacker Tracker](#), or the nearest NFO Node for the latest.

Sunday - 00:00 PDT

[Return to Index](#) - [Locations Legend](#)

[Social Gatherings/Events](#) - [Music](#) - [Genre: Drum & Bass](#) - [DJ XORAC](#)

Sunday - 08:00 PDT

[Return to Index](#) - [Locations Legend](#)

[DEF CON Training](#) - (08:30-17:30 PDT) - [Blue vs Red Bootcamp: From Attacker Playbooks to Defender Detections](#) - Carlo Anez Mazurco,Mariana Ruiz

[DEF CON Training](#) - (08:30-17:30 PDT) - [Influence Operations: Tactics, Defense, and Exploitation](#) - Greg Conti,Tom Cross

[DEF CON Training](#) - (08:30-17:30 PDT) - [Full-Stack Pentesting Laboratory: 100% Hands-On + Lifetime LAB Access](#) - Dawid Czagan

[Return to Index](#) - [Locations Legend](#)

[DEF CON Training](#) - cont...(08:30-17:30 PDT) - [Blue vs Red Bootcamp: From Attacker Playbooks to Defender Detections](#) - Carlo Anez Mazurco,Mariana Ruiz

[DEF CON Training](#) - cont...(08:30-17:30 PDT) - [Influence Operations: Tactics, Defense, and Exploitation](#) - Greg Conti,Tom Cross

[DEF CON Training](#) - cont...(08:30-17:30 PDT) - [Full-Stack Pentesting Laboratory: 100% Hands-On + Lifetime LAB Access](#) - Dawid Czagan

[DEF CON Workshops](#) - [Sold Out](#) - [Attacking Cloud APIs from the IoT Edge](#) - Rodney "BenevolentWorm" Beede

[DEF CON Workshops](#) - [Sold Out](#) - [Building your own hardware hacking kit to Pentest Bluetooth, WIFI, and more.](#) - Dallas

[DEF CON Workshops](#) - [Sold Out](#) - [Post-Quantum Cryptography \(PQC\) for Hackers](#) - Eric "Eijah" Anderson

[DEF CON Workshops](#) - [Sold Out](#) - [Purple Protocol: Adversary emulation for everyone](#) - Patrick "PilotPat" Raiden,Ben "Marba\$" Strout,Brandon "D43m0n" Kraycirik

[DEF CON Workshops](#) - [Sold Out](#) - [CI/CD Weaponization: Build It, Deploy It, Own It](#) - Ricardo Sanchez,Daniel Malvaceda

[DEF CON Workshops](#) - [Sold Out](#) - [ICS Hack 'n Track](#) - Pedro Cabrera,Hannes "hercules_hannes" Heck,Sam Miorelli,Jordan Sanchez

[DEF CON Workshops](#) - [Sold Out](#) - [Creating Shellcode for Hackers](#) - Bramwell "Bw3ll" Brizendine,Austin "quantumite" Norby,Micah Flack

[DEF CON Workshops](#) - [Sold Out](#) - [Pivot, Hunt, Publish: An Offline, Hands-On CTI Workshop for Blue Teams and Threat Researchers](#) - Rushikesh Nandedkar

[Social Gatherings/Events](#) - [Human Registration Open](#) -

[Return to Index](#) - [Locations Legend](#)

[Aerospace Village](#) - [DCNextGen](#) - [Bricks in the Air](#) -
[Aerospace Village](#) - [DCNextGen](#) - [Space Grand Challenge](#) - [SatHack: The MOUSE-1 Mission](#) -
[Aerospace Village](#) - [DCNextGen](#) - [RIC-1: ELT Localization Exercise](#) - [N3VR-G0N Down](#) -
[Aerospace Village](#) - [Bricks in the Air](#) -
[Aerospace Village](#) - [Aviation ISAC Cybersecurity Challenge](#) -
[Aerospace Village](#) - [Aerospace Ecosystem Resilience Innovation Environment \(AERIE\) Cyber Range](#) -
[Aerospace Village](#) - [ARINC 664 CTF Challenge](#) -
[Aerospace Village](#) - [SR-71 Blackbird Badge Challenge](#) -
[Aerospace Village](#) - [SpaceCOP](#) - [Catch Me If You Can](#) -
[Aerospace Village](#) - [Satellites Under Attack: Hands-On Satellite Security Threat Scenarios](#) -
[Aerospace Village](#) - [Nebula Showdown: Space Systems Security CTF Adventure](#) -
[Aerospace Village](#) - [MOUSE Runner & Flappy Drone](#) -
[Aerospace Village](#) - [Flight Simulator/EFB](#) -
[Aerospace Village](#) - [Drone Hacking Choose your Own Adventure](#) -
[Aerospace Village](#) - [Drone Hacking Workshop](#) -
[Aerospace Village](#) - [Mission: Compromised](#) - [Hacking a Satellite from the Ground Up](#) -
[AI Village](#) - [AI Village: Village Open](#) -
[AI Village](#) - [Cyber Mirage: Realtime Deepfake Demos](#) - [Brandon Kovacs](#)
[AI Village](#) - [A Billion-User Blast Radius: Owning ChatGPT's Secure Sandbox](#) - [Simcha Kosman](#)
[AI Village](#) - (10:30-10:59 PDT) - [Scaling Adversary Emulation with Autonomous Agents](#) - [Daniel Fabien](#)
[AppSec Village](#) - (10:15-11:15 PDT) - [ROP for the Web: Smuggling XSS, SQLi, and Web Shells Past Every WAF Using Compression Dictionaries](#) - [alevsk](#)
[AppSec Village](#) - (10:15-12:59 PDT) - [Introduction to AI-Enhanced Threat Modeling Workshop](#) - [Robert Hurlbut](#)
[AppSec Village](#) - (10:30-10:59 PDT) - [From commit to compromise: securing the full pipeline with AI-assisted remediation](#) - [Filipi Pires](#)
[Biohacking Village](#) - [Embedded & Shredded: Advanced Embedded System Hacking](#) -
[Biohacking Village](#) - [Biohacking Device Lab](#) -
[Biohacking Village](#) - (10:30-10:59 PDT) - [Wand Protocol: Full-Chain Attack on an FDA-Listed Fertility Analyzer](#) - [Gigi Xiaoqing Liu](#)
[Blacks In Cyber Village](#) - [From Practitioner to Principal: Building a Cybersecurity Business That Lasts](#) - [Tyrone E. Wilson](#)
[Bug Bounty Village](#) - [Skill Issue: A Recon Story](#) - [Ryan Bonner](#)
[Bug Bounty Village](#) - (10:30-10:59 PDT) - [Slop Spotting, Using Rules to Detect AI Slop for Bug Bounty](#) - [Katie Paxton-Fear,Max vonBlankenburg](#)
[Bug Bounty Village](#) - [AI Cuts Both Ways: Using AI to Find More Bugs, and Finding the New Bugs AI Creates](#) - [Ciarán "monke" Cotter](#)
[Call Center Village](#) - [Call Center Village](#) - [Open](#) -
[Car Hacking Village](#) - [Car Hacking Village Open](#) -
[Car Hacking Village](#) - (10:30-10:59 PDT) - [Unlocking Vehicles by Brute-Forcing Rolling Code Systems](#) - [Danilo Erazo](#)
[Cloud Village](#) - [Tag, You're It: Authorization Traps in AWS ABAC](#) - [Itay Saraf](#)
[Cloud Village](#) - (10:40-11:20 PDT) - [When Machines Attack Machines: Detecting AI-Autonomous Cloud Compromise at NHI Scale](#) - [Gowthamaraj Rajendran](#)
[CodeBloom](#) - [Game Time: Loops](#) -
[Contests](#) - [5N4CK3Y](#) -
[Contests](#) - [DC's Next Top Threat Model](#) -
[Contests](#) - [Untechnical](#) -
[Contests](#) - [DEF CON Scavenger Hunt](#) -
[Contests](#) - [Darknet-NG](#) -
[Contests](#) - [Crack Me If You Can 2026](#) -
[Contests](#) - [TeleChallenge](#) -
[Contests](#) - [HackFortress](#) -
[Contests](#) - [?Cube](#) -

[Contests - \\$unLight Sh4d0w5 -](#)
[Contests - Beer Chilling Contraption Contest -](#)
[Contests - Cryptid Hunt -](#)
[Contests - HSPACE: AI Battlegrounds -](#)
[Contests - spyVspy 3: Rat Race -](#)
[Contests - Hacker Games -](#)
[Contests - PhreakMe -](#)
[Contests - Game Hacking Village CTF awards ceremony -](#)
[Contests - Game Hacking Village CTF Q&A / Walkthroughs -](#)
[Contests - Kubernetes CTF -](#)
[Contests - Hac-Man -](#)
[Contests - Crack the Core -](#)
[Contests - Cyber Deck Competition -](#)
[Contests - Pinball High Score Contest -](#)
[Contests - Code Cadaver: Break Every System. Save Your Friend. -](#)
[Contests - PWN UR H0M3 - DDoS CTF -](#)
[Contests - Reali7y Overrun - Contest running -](#)
[Contests - Tin Foil Hat Contest -](#)
[Contests - CMD+CTRL Cyber Range: DarkMoney -](#)
[Contests - Radio Frequency Capture the Flag -](#)
[Contests - DEF CON CTF: Benevolent Bureau of Birds -](#)
[Contests - AI Village - Hal CTF -](#)
[Contests - AI Village Plays Pokemon: DEFCON Edition - Nick Ashworth](#)
[Contests - Car Hacking Village CTF -](#)
[Contests - Escalation Desk CTF -](#)
[Contests - Contest Awards -](#)
[Contests - Hacking GRC Contest -](#)
[Data Duplication Village - Last chance to pick up drives at the DDV -](#)
[DCNextGen - Cloud Village CTF: Three Azure Warmups - Cloud Village](#)
[DEF CON Groups - Lessons Learned from Building a New DEF CON Group presented by DC724 - Cliff "GritsnGravy" Friedel, Joe "jbohack"](#)
[DEF CON Groups - DEF CON Groups \(DCG\) -](#)
[DEF CON Talks - ESP32 as a counter-surveillance platform - Cooper "Cybertiger" Quintin, Colonel Panic, The Wrew](#)
[DEF CON Talks - This Message Was Sent by Microsoft: Turning Microsoft Apps into our Phishing Platform - Keanu "RedByte" Nys](#)
[DEF CON Talks - Shepherd the Tor network - Roger "arma" Dingledine](#)
[DEF CON Talks - Going the Distance: Long-Range Keystroke Injection via Meshtastic - Benito "paperclipsvinny" Saucedo](#)
[DEF CON Talks - \(10:30-11:30 PDT\) - Reversing a Recall: From 'Noise Triggered' to RCE - Ben Gardiner](#)
[DEF CON Talks - No Prompt Required: Pre-Task RCE in Google Gemini CLI - Elad Meged](#)
[DEF CON Talks - \(10:30-11:30 PDT\) - Gotta Phish 'Em All! Novel Attack Techniques via Persistent Browser-in-the-Middle - Giacomo "GiacLenzo2109" Lenzini](#)
[DEF CON Training - cont...\(08:30-17:30 PDT\) - Blue vs Red Bootcamp: From Attacker Playbooks to Defender Detections - Carlo Anez Mazurco, Mariana Ruiz](#)
[DEF CON Training - cont...\(08:30-17:30 PDT\) - Influence Operations: Tactics, Defense, and Exploitation - Greg Conti, Tom Cross](#)
[DEF CON Training - cont...\(08:30-17:30 PDT\) - Full-Stack Pentesting Laboratory: 100% Hands-On + Lifetime LAB Access - Dawid Czagan](#)
[DEF CON Workshops - cont...\(09:00-12:59 PDT\) - Sold Out - Attacking Cloud APIs from the IoT Edge - Rodney "BenevolentWorm" Beede](#)
[DEF CON Workshops - cont...\(09:00-12:59 PDT\) - Sold Out - Building your own hardware hacking kit to Pentest Bluetooth, WIFI, and more. - Dallas](#)
[DEF CON Workshops - cont...\(09:00-12:59 PDT\) - Sold Out - Post-Quantum Cryptography \(PQC\) for Hackers - Eric "Eijah" Anderson](#)
[DEF CON Workshops - cont...\(09:00-12:59 PDT\) - Sold Out - Purple Protocol: Adversary emulation for everyone - Patrick "PilotPat" Raiden, Ben "Marba\\$" Strout, Brandon "D43m0n" Kraycirik](#)

DEF CON Workshops - cont...(09:00-12:59 PDT) - Sold Out - CI/CD Weaponization: Build It, Deploy It, Own It - Ricardo Sanchez, Daniel Malvaceda

DEF CON Workshops - cont...(09:00-12:59 PDT) - Sold Out - ICS Hack 'n Track - Pedro Cabrera, Hannes "hercules_hannes" Heck, Sam Miorelli, Jordan Sanchez

DEF CON Workshops - cont...(09:00-12:59 PDT) - Sold Out - Creating Shellcode for Hackers - Bramwell "Bw3ll" Brizendine, Austin "quantumite" Norby, Micah Flack

DEF CON Workshops - cont...(09:00-12:59 PDT) - Sold Out - Pivot, Hunt, Publish: An Offline, Hands-On CTI Workshop for Blue Teams and Threat Researchers - Rushikesh Nandedkar

Embedded Systems Village - Exploit Bluetooth Low Energy with BLESpoit and optional ESP32 - Slawomir Jasek

Embedded Systems Village - Embedded Systems Village CTF -

Embedded Systems Village - Embedded - 101 Labs -

Hackers.town - (10:30-10:59 PDT) - The Enshittified Internet and How We Can All Rewild the Internet - LambdaCalculus

Ham Radio Village - "Can it Ham" Antenna Testing - The HRV Contest Team

ICS Village - Five Million Industrial Control Systems Walk Into a Bar: What IRONMAP Found When It Scanned the Whole Internet - Matt Caldwell

IoT Village - Just Hacking Training -

IoT Village - Raiders of the Lost Firmware: A Hands-On Workshop in IoT Firmware Archaeology -

IoT Village - Hands-On Hardware Hacking – From JTAG to Root, Memory Patching Boot Process for Root Access -

IoT Village - Cat-astrophic Hacking: Breaking Into Smart Litter Boxes -

IoT Village - Smart Home in the Matter: Blink, Race, Attack CTF -

IoT Village - Discover GE Appliances! -

IoT Village - Expose Hidden Surveillance in Everyday Tech -

IoT Village - All About UART -

IoT Village - (10:15-10:59 PDT) - Make your very own evil IoT Cat Lamp with WLED! - Nick

IoT Village - You Can't Opt Out: The Invisible Surveillance in Your Walls, Pockets, and Lives - Naomi Brockwell

La Villa Community - Tu foco IoT nunca tuvo modelo de amenazas - Andres Sabas

La Villa Community - (10:30-11:30 PDT) - Bait the Bot: Hacking Back Autonomous AI Vulnerability Scanners - Alcyon Junior

Lockpick Village - (10:15-10:45 PDT) - Intro to Lockpicking -

Lonely Hackers Club - Lonely Hackers Club - Lockpicking Table -

Lonely Hackers Club - Lonely Hackers Club CTF -

Lonely Hackers Club - Lonely Hackers Club - Sticker Swap Table -

Maker's Village - Makers' Village - Hacker Arts and Crafts -

Middle Easterns & Africans in Cyber Security (MEACS) - From Roots to Renaissance: The Rising Generation of Middle Eastern and African Cybersecurity - Ezz Tahoun

Misc - Coloring Reset -

Mobile Hacking Community - Mobile Hacking Community - Open -

Mobile Hacking Community - Mobile Hacking - Informal CTF -

Noob Community - Break Things, Learn Things: Hands-On Hacking for Beginners (same as Saturday) - Evolve Security Academy

Noob Community - Arcanum Security Labs -

Noob Community - Mentoring and Career Advice -

Noob Community - Kryptsec Labs -

Noob Community - No Stupid Questions -

Noob Community - Hack The Box DC Junior Ranger Program Challenge -

Noob Community - Skillbit Labs -

Noob Community - SANS Institute NetWars Labs -

Noob Community - TCM Security Labs -

Noob Community - (10:30-11:30 PDT) - Ctrl + Alt + Lead: Rebooting Cyber Culture with Human Skills - Amanda Kollmorgan

OSINT For Good Community - OSINT4Good Community - DC NextGen Content -

OSINT For Good Community - FINDX OSINT Educational Series -

OSINT For Good Community - (10:30-10:59 PDT) - How to Profile an entire C-suite in 10 days - Sarah Muriel

OWASP Foundation - Spotlight: Choose Your Own Adventure with InfoSecMap - W. Martín Villalba

OWASP Foundation - (10:30-12:30 PDT) - 2001: Agentic Odyssey in Threat Modeling - Petra Vukmirovic

[Payment Village](#) - (10:30-10:50 PDT) - [Wall of Wallets Workshop \(Intro to Wall of Wallets Challenge\)](#) - Dan Borgogno
[Physical Security Village](#) - [Breaking In, Evil Style: A Guide to Scaring Your CEO](#) - Andrew Lebedinsky
[Radio Frequency Village](#) - [WarDriver Meetup](#) -
[Radio Frequency Village](#) - [Radio Frequency Village Events](#) -
[Recon Village](#) - [Ghost in the Hiring Machine: How to Spot Fake Personas Before They're on Your Payroll](#) - Michael Reimsbach,Rishi "rxerium" C
[Recon Village](#) - (10:45-11:30 PDT) - [Living Off Someone Else's Inference](#) - Redon Gashi,Armend Gashi
[Red Team Village](#) - [Attack Campaign in VR](#) - James Rice
[Red Team Village](#) - [Tokens and PRT: Advanced Attacks and Persistence in Microsoft Entra ID](#) - Elzer Pineda,Jose Rivas
[Red Team Village](#) - [0-Day Hunting Table: Come Join the Vulnpocalypse](#) - Chris Haller
[Red Team Village](#) - [Evil Is Always a Bad Stylist: .NET Obfuscation with Roslyn](#) - Alexander Rodchenko,Ashley Hiram Muñoz,Eduardo Chavarro Ovalle
[Red Team Village](#) - [Beyond NPPSPY: Harvesting Credentials via Windows Credential Provider Framework](#) - Sohail Saha
[Red Team Village](#) - [Beyond the Flag: How CTF Players Become Product Security Engineers](#) - Drew Thompson,Monish Alur Gowdru
[Red Team Village](#) - [Direct Network Access for Command and Control](#) - Andrew Rioux
[Scambait Village](#) - [Open Q&A](#) -
[Scambait Village](#) - [Scambait Bingo](#) -
[Scambait Village](#) - [KSCM Scambait Radio](#) -
[Social Engineering Community Village](#) - [Social Engineering Community Village](#) - [Open Hours](#) -
[Social Engineering Community Village](#) - (10:30-11:30 PDT) - [2027 SECVC Pre-Qualification Round - LIVE CALLS](#) -
[Social Gatherings/Events](#) - cont...(09:00-11:59 PDT) - [Human Registration Open](#) -
[Social Gatherings/Events](#) - [Music](#) - SomaFM -
[Telecom Village](#) - (10:20-13:59 PDT) - [Telecom Village CTF](#) - T -Mobile CTF Team
[The Diana Initiative](#) - [The Diana Initiative](#) - [Open time](#) -
[Voting Village](#) - [Voting Village Lab](#) -

[Adversary Village - Beyond the Hype: The Real Role of Red Teams in an AI World](#) - Michael Leibowitz,Niranjanaa Ragupathy

[Aerospace Village - cont...\(10:00-13:59 PDT\) - MOUSE Runner & Flappy Drone](#) -

[Aerospace Village - cont...\(10:00-13:59 PDT\) - Mission: Compromised - Hacking a Satellite from the Ground Up](#) -

[Aerospace Village - cont...\(10:00-13:59 PDT\) - Drone Hacking Choose your Own Adventure](#) -

[Aerospace Village - cont...\(10:00-13:59 PDT\) - Flight Simulator/EFB](#) -

[Aerospace Village - cont...\(10:00-13:59 PDT\) - Drone Hacking Workshop](#) -

[Aerospace Village - cont...\(10:00-13:59 PDT\) - SR-71 Blackbird Badge Challenge](#) -

[Aerospace Village - cont...\(10:00-13:59 PDT\) - Satellites Under Attack: Hands-On Satellite Security Threat Scenarios](#) -

[Aerospace Village - cont...\(10:00-13:59 PDT\) - Nebula Showdown: Space Systems Security CTF Adventure](#) -

[Aerospace Village - cont...\(10:00-13:59 PDT\) - SpaceCOP - Catch Me If You Can](#) -

[Aerospace Village - cont...\(10:00-13:59 PDT\) - Aviation ISAC Cybersecurity Challenge](#) -

[Aerospace Village - cont...\(10:00-13:59 PDT\) - Aerospace Ecosystem Resilience Innovation Environment \(AERIE\) Cyber Range](#) -

[Aerospace Village - cont...\(10:00-13:59 PDT\) - ARINC 664 CTF Challenge](#) -

[Aerospace Village - cont...\(10:00-13:59 PDT\) - DCNextGen - Space Grand Challenge - SatHack: The MOUSE-1 Mission](#) -

[Aerospace Village - cont...\(10:00-13:59 PDT\) - DCNextGen - RIC-1: ELT Localization Exercise - N3VR-G0N Down](#) -

[Aerospace Village - cont...\(10:00-13:59 PDT\) - DCNextGen - Bricks in the Air](#) -

[Aerospace Village - cont...\(10:00-13:59 PDT\) - Bricks in the Air](#) -

[AI Village - cont...\(10:00-13:59 PDT\) - AI Village: Village Open](#) -

[AI Village - cont...\(10:00-13:59 PDT\) - Cyber Mirage: Realtime Deepfake Demos](#) - Brandon Kovacs

[AI Village - What is AI? Interactive, Unplugged Activity](#) - Sam Mosley

[AppSec Village - cont...\(10:15-11:15 PDT\) - ROP for the Web: Smuggling XSS, SQLi, and Web Shells Past Every WAF Using Compression Dictionaries](#) - alevsk

[AppSec Village - \(11:30-12:30 PDT\) - search_vulns: Navigating the Fragmented Landscape of Vulnerability Data](#) - Dustin Born,Matthias Göhring

[AppSec Village - cont...\(10:15-12:59 PDT\) - Introduction to AI-Enhanced Threat Modeling Workshop](#) - Robert Hurlbut

[AppSec Village - Extending Shared Threat Models with the Application Attack Matrix](#) - J Fridley

[AppSec Village - \(11:50-12:20 PDT\) - Finding Bugs Is Easy, Patching Isn't: Build Your Own Remediation Pipeline](#) - Mohan Kumar,Naveen

[AppSec Village - Clash of Prompts: The World's First Prompt Battle Royale](#) - Darren McNelis,Jerome Roberts

[AppSec Village - AppSec Quiz Gauntlet: Spot the Vulnerability](#) - Avek Kolech

[AppSec Village - SBOM Find the Flaws](#) - Dmitry Raidman

[AppSec Village - NPM Imposters - The malware detection card game](#) - Mackenzie

[Biohacking Village - cont...\(10:00-13:59 PDT\) - Embedded & Shredded: Advanced Embedded System Hacking](#) -

[Biohacking Village - cont...\(10:00-13:59 PDT\) - Biohacking Device Lab](#) -

[Blacks In Cyber Village - Quantum Computing The Game Changer You Can t Ignore](#) - Danielle Eason

[Blue Team Village - You're Hired... Maybe: Inside Cybersecurity Hiring in 2026](#) - George Scheibe,Neha Gautam,Sherry Michael,Siddharth Kumar

[Bug Bounty Village - \(11:30-11:59 PDT\) - Automated Discovery of Prompt Injection Vulnerabilities via Mutated Prompt Generation](#) - Bogdan Steele,Arnav Garg

[Bug Bounty Village - Full Disclosure, Full Screen: \[Informative\] The Story of Bug Bounty Village Badge 2026](#) - Abhinav "TweetsFromPanda" Pandagale

[Bug Bounty Village - \(11:30-11:59 PDT\) - Heavy Metal and Hidden Secrets: A Five-Year Retrospective on DEF CON Challenge Coins](#) - Ariel "arl_rose" Garcia

[Call Center Village - cont...\(10:00-13:59 PDT\) - Call Center Village - Open](#) -

[Car Hacking Village - cont...\(10:00-13:59 PDT\) - Car Hacking Village Open](#) -

[Car Hacking Village - \(11:30-11:59 PDT\) - Stealing at the Speed of Light: The Anatomy of a Real Relay Attack tool](#) - Robbie Galfrin

[Cloud Village - The Autonomous Insider](#) - Naveen Reddy Pogalla,Hari Pranav Arun Kumar

[Cloud Village - cont...\(10:40-11:20 PDT\) - When Machines Attack Machines: Detecting AI-Autonomous Cloud Compromise](#)

at NHI Scale - Gowthamaraj Rajendran

Cloud Village - (11:20-11:50 PDT) - [Breaking the Oracle: Building an Offensive Security Toolkit for OCI](#) - Scott Weston

Cloud Village - (11:50-12:30 PDT) - [Foxveil: Cloud-Native Loader Tradecraft on Cloudflare, Netlify, and Discord](#) - Shani

Kurtzberg,Zohar Buber

CodeBloom - [Work Session: Ciphers](#) -

Contests - cont...(10:00-11:59 PDT) - [5N4CK3Y](#) -

Contests - cont...(10:00-11:59 PDT) - [DC's Next Top Threat Model](#) -

Contests - cont...(10:00-11:59 PDT) - [Untechnical](#) -

Contests - cont...(10:00-11:59 PDT) - [DEF CON Scavenger Hunt](#) -

Contests - cont...(10:00-11:59 PDT) - [Darknet-NG](#) -

Contests - cont...(10:00-11:59 PDT) - [Crack Me If You Can 2026](#) -

Contests - cont...(10:00-11:59 PDT) - [TeleChallenge](#) -

Contests - cont...(10:00-11:59 PDT) - [HackFortress](#) -

Contests - cont...(10:00-11:59 PDT) - [?Cube](#) -

Contests - cont...(10:00-11:59 PDT) - [\\$unLight Sh4d0w5](#) -

Contests - cont...(10:00-11:59 PDT) - [Beer Chilling Contraption Contest](#) -

Contests - cont...(10:00-11:59 PDT) - [Cryptid Hunt](#) -

Contests - cont...(10:00-11:59 PDT) - [HSPACE: AI Battlegrounds](#) -

Contests - cont...(10:00-11:59 PDT) - [spyVspy 3: Rat Race](#) -

Contests - cont...(10:00-11:59 PDT) - [Hacker Games](#) -

Contests - cont...(10:00-11:59 PDT) - [PhreakMe](#) -

Contests - cont...(10:00-11:59 PDT) - [Game Hacking Village CTF Q&A / Walkthroughs](#) -

Contests - cont...(10:00-11:59 PDT) - [Kubernetes CTF](#) -

Contests - cont...(10:00-11:59 PDT) - [Hac-Man](#) -

Contests - cont...(10:00-11:59 PDT) - [Crack the Core](#) -

Contests - cont...(10:00-11:59 PDT) - [Cyber Deck Competition](#) -

Contests - cont...(10:00-11:59 PDT) - [Pinball High Score Contest](#) -

Contests - cont...(10:00-13:59 PDT) - [Code Cadaver: Break Every System. Save Your Friend.](#) -

Contests - cont...(10:00-11:59 PDT) - [PWN UR H0M3 - DDoS CTF](#) -

Contests - cont...(10:00-11:59 PDT) - [Real7y Overrun - Contest running](#) -

Contests - cont...(10:00-11:59 PDT) - [Tin Foil Hat Contest](#) -

Contests - cont...(10:00-12:59 PDT) - [CMD+CTRL Cyber Range: DarkMoney](#) -

Contests - cont...(10:00-11:59 PDT) - [DEF CON CTF: Benevolent Bureau of Birds](#) -

Contests - cont...(10:00-13:59 PDT) - [AI Village - Hal CTF](#) -

Contests - cont...(10:00-13:59 PDT) - [AI Village Plays Pokemon: DEFCON Edition](#) - Nick Ashworth

Contests - cont...(10:00-11:59 PDT) - [Car Hacking Village CTF](#) -

Contests - cont...(10:00-11:59 PDT) - [Escalation Desk CTF](#) -

Contests - cont...(10:00-11:59 PDT) - [Hacking GRC Contest](#) -

Crypto & Privacy Village - [Cove: Compositional and Verifiable Confidential Computing Workflows](#) - Stephanie,Robin,Erika Lee

Cryptocurrency Village - [Cryptocurrency Closing Keynote](#) - Chelsea Button,Param "P7R7M",Arjun "Peper" Suresh

DEF CON Groups - [The State of DEF CON Groups](#) - Alethe Denis,Magen Wu

DEF CON Groups - cont...(10:00-13:59 PDT) - [DEF CON Groups \(DCG\)](#) -

DEF CON Talks - [LaunchBreak: a Sip of Tea, a Click, and a Full Multi-stage Desktop Takeover](#) - Gavin Zhong,Zhengyu Liu,Jianjia Yu

DEF CON Talks - [Beyond the Ceremony: The 2026 Passkey Attack Surface](#) - Matteo Giordano

DEF CON Talks - [Gone in 60 Frames – USB Video Exploitation](#) - Alex Plaskett,Robert Herrera

DEF CON Talks - cont...(10:30-11:30 PDT) - [Reversing a Recall: From ‘Noise Triggered’ to RCE](#) - Ben Gardiner

DEF CON Talks - (11:30-12:30 PDT) - [BLE Theft Auto: How a Dealer-Installed Anti-Theft System Exposes Over a Million Cars to Theft](#) - Aaron Schulman,Jerry Yu,Yibo Wei

DEF CON Talks - cont...(10:30-11:30 PDT) - [Gotta Phish 'Em All! Novel Attack Techniques via Persistent](#)

[Browser-in-the-Middle](#) - Giacomo "GiaccoLenzo2109" Lenzini

DEF CON Talks - (11:30-12:30 PDT) - [From Fuzzer Noise to a Weaponized PHP Exploit: Exploiting a PHP Use-After-Free Vulnerability](#) - Can Oztas,Kağan Çapar

DEF CON Training - cont...(08:30-17:30 PDT) - [Blue vs Red Bootcamp: From Attacker Playbooks to Defender Detections](#) -

Carlo Anez Mazurco,Mariana Ruiz

[DEF CON Training](#) - cont...(08:30-17:30 PDT) - [Influence Operations: Tactics, Defense, and Exploitation](#) - Greg Conti,Tom Cross

[DEF CON Training](#) - cont...(08:30-17:30 PDT) - [Full-Stack Pentesting Laboratory: 100% Hands-On + Lifetime LAB Access](#) - Dawid Czagan

[DEF CON Workshops](#) - cont...(09:00-12:59 PDT) - [Sold Out - Attacking Cloud APIs from the IoT Edge](#) - Rodney "BenevolentWorm" Beede

[DEF CON Workshops](#) - cont...(09:00-12:59 PDT) - [Sold Out - Building your own hardware hacking kit to Pentest Bluetooth, WIFI, and more.](#) - Dallas

[DEF CON Workshops](#) - cont...(09:00-12:59 PDT) - [Sold Out - Post-Quantum Cryptography \(PQC\) for Hackers](#) - Eric "Eijah" Anderson

[DEF CON Workshops](#) - cont...(09:00-12:59 PDT) - [Sold Out - Purple Protocol: Adversary emulation for everyone](#) - Patrick "PilotPat" Raiden,Ben "Marba\$" Strout,Brandon "D43m0n" Kraycirik

[DEF CON Workshops](#) - cont...(09:00-12:59 PDT) - [Sold Out - CI/CD Weaponization: Build It, Deploy It, Own It](#) - Ricardo Sanchez,Daniel Malvaceda

[DEF CON Workshops](#) - cont...(09:00-12:59 PDT) - [Sold Out - ICS Hack 'n Track](#) - Pedro Cabrera,Hannes "hercules_hannes" Heck,Sam Miorelli,Jordan Sanchez

[DEF CON Workshops](#) - cont...(09:00-12:59 PDT) - [Sold Out - Creating Shellcode for Hackers](#) - Bramwell "Bw3ll" Brizendine,Austin "quantumite" Norby,Micah Flack

[DEF CON Workshops](#) - cont...(09:00-12:59 PDT) - [Sold Out - Pivot, Hunt, Publish: An Offline, Hands-On CTI Workshop for Blue Teams and Threat Researchers](#) - Rushikesh Nandedkar

[Embedded Systems Village](#) - cont...(10:00-13:59 PDT) - [Exploit Bluetooth Low Energy with BLESPlloit and optional ESP32](#) - Slawomir Jasek

[Embedded Systems Village](#) - cont...(10:00-13:59 PDT) - [Embedded Systems Village CTF](#) -

[Embedded Systems Village](#) - cont...(10:00-13:59 PDT) - [Embedded - 101 Labs](#) -

[Game Hacking Village](#) - (11:30-12:30 PDT) - [Yes, I froze an SNES for science](#) - dwangoAC

[Ham Radio Village](#) - cont...(10:00-11:30 PDT) - ["Can it Ham" Antenna Testing](#) - The HRV Contest Team

[ICS Village](#) - [Is Your Fridge Running? Then You Better Catch It](#) - State of Security in Refrigeration Systems - Amir Zaltzman

[IoT Village](#) - cont...(10:00-13:59 PDT) - [All About UART](#) -

[IoT Village](#) - cont...(10:00-13:59 PDT) - [Smart Home in the Matter: Blink, Race, Attack CTF](#) -

[IoT Village](#) - cont...(10:00-13:59 PDT) - [Discover GE Appliances!](#) -

[IoT Village](#) - cont...(10:00-13:59 PDT) - [Expose Hidden Surveillance in Everyday Tech](#) -

[IoT Village](#) - cont...(10:00-13:59 PDT) - [Raiders of the Lost Firmware: A Hands-On Workshop in IoT Firmware Archaeology](#) -

[IoT Village](#) - cont...(10:00-13:59 PDT) - [Hands-On Hardware Hacking – From JTAG to Root, Memory Patching Boot Process for Root Access](#) -

[IoT Village](#) - cont...(10:00-13:59 PDT) - [Cat-astrophic Hacking: Breaking Into Smart Litter Boxes](#) -

[IoT Village](#) - cont...(10:00-13:59 PDT) - [Just Hacking Training](#) -

[IoT Village](#) - [Wi-Fi Self Defense & Hacker Hunting & For Beginners](#) - Kody Kinzie

[IoT Village](#) - (11:30-11:59 PDT) - [One Firmware Flaw, 70+ Device Models: Lessons in Industrial IoT Disclosure and Mitigation](#) - Weihan Goh,ZhengChao Wen

[La Villa Community](#) - cont...(10:30-11:30 PDT) - [Bait the Bot: Hacking Back Autonomous AI Vulnerability Scanners](#) - Alcyon Junior

[La Villa Community](#) - (11:30-11:59 PDT) - [La Rosa de Guadalupe DFIR: Serie de 3 capítulos de misterio Cyber*](#) - Victor Gomez,Horacio Bazán

[Lockpick Village](#) - [The Knox Box - A Brief History\(Part II\)](#) - Matthew O'Reilly

[Lonely Hackers Club](#) - cont...(10:00-13:59 PDT) - [Lonely Hackers Club - Sticker Swap Table](#) -

[Lonely Hackers Club](#) - cont...(10:00-13:59 PDT) - [Lonely Hackers Club - Lockpicking Table](#) -

[Lonely Hackers Club](#) - cont...(10:00-11:59 PDT) - [Lonely Hackers Club CTF](#) -

[Maker's Village](#) - cont...(10:00-13:59 PDT) - [Makers' Village - Hacker Arts and Crafts](#) -

[Maker's Village](#) - [3d Designing basics, 5 minute prints in Tinkercad](#) - hunny

[Mobile Hacking Community](#) - (11:30-11:59 PDT) - [IsMyPhonePwned: Analyzing Android/iOS Phones at Scale](#) - Desnos Anthony

[Mobile Hacking Community](#) - cont...(10:00-13:59 PDT) - [Mobile Hacking Community - Open](#) -

[Mobile Hacking Community](#) - cont...(10:00-11:59 PDT) - [Mobile Hacking - Informal CTF](#) -

[Noob Community](#) - cont...(10:00-13:59 PDT) - [No Stupid Questions](#) -
[Noob Community](#) - cont...(10:00-13:59 PDT) - [Mentoring and Career Advice](#) -
[Noob Community](#) - cont...(10:00-13:59 PDT) - [Kryptsec Labs](#) -
[Noob Community](#) - cont...(10:00-13:59 PDT) - [Hack The Box DC Junior Ranger Program Challenge](#) -
[Noob Community](#) - cont...(10:00-13:59 PDT) - [Arcanum Security Labs](#) -
[Noob Community](#) - cont...(10:00-13:59 PDT) - [SANS Institute NetWars Labs](#) -
[Noob Community](#) - cont...(10:00-13:59 PDT) - [TCM Security Labs](#) -
[Noob Community](#) - cont...(10:00-13:59 PDT) - [Skillbit Labs](#) -
[Noob Community](#) - cont...(10:30-11:30 PDT) - [Ctrl + Alt + Lead: Rebooting Cyber Culture with Human Skills](#) - Amanda Kollmorgan
[Noob Community](#) - [From Command Line to Center Stage: Hack Your Way to Confident Speaking](#) - James McQuiggan
[Noob Community](#) - (11:45-12:15 PDT) - [So You Want to Be a Red Teamer? The Reality Behind the Role](#) - Billy Giles
[OSINT For Good Community](#) - cont...(10:00-13:59 PDT) - [FINDX OSINT Educational Series](#) -
[OSINT For Good Community](#) - cont...(10:00-13:59 PDT) - [OSINT4Good Community - DC NextGen Content](#) -
[OSINT For Good Community](#) - [Q&A with the "How to Profile an entire C-suite in 10 days" speaker](#) - Sarah Muriel
[OSINT For Good Community](#) - (11:30-12:45 PDT) - [Disaster Intelligence - The past, present, and future of situational awareness during a crisis](#) - Matt Green
[OSINT For Good Community](#) - (11:30-11:59 PDT) - [Disaster Intelligence - The past, present, and future of situational awareness during a crisis](#) - Matt Green
[OWASP Foundation](#) - cont...(10:30-12:30 PDT) - [2001: Agentic Odyssey in Threat Modeling](#) - Petra Vukmirovic
[OWASP Foundation](#) - [OWASP Chapter Meetup](#) -
[Physical Security Village](#) - [Physical Security is not sexy which is bad for organizations and good for red teams.](#) - Roger Egan
[Policy @ DEF CON](#) - [Strategic Resistance: How a Global Network is Fighting the Spyware Industry](#) - - Michael Brennan,Nadine Farid Johnson,Rebekah Brown
[Radio Frequency Village](#) - cont...(10:00-13:59 PDT) - [Radio Frequency Village Events](#) -
[Radio Frequency Village](#) - cont...(10:00-11:55 PDT) - [WarDriver Meetup](#) -
[Recon Village](#) - cont...(10:45-11:30 PDT) - [Living Off Someone Else's Inference](#) - Redon Gashi,Armend Gashi
[Red Team Village](#) - cont...(10:00-14:59 PDT) - [Attack Campaign in VR](#) - James Rice
[Red Team Village](#) - cont...(10:00-11:59 PDT) - [Tokens and PRT: Advanced Attacks and Persistence in Microsoft Entra ID](#) - Elzer Pineda,Jose Rivas
[Red Team Village](#) - cont...(10:00-11:59 PDT) - [0-Day Hunting Table: Come Join the Vulnpocalypse](#) - Chris Haller
[Red Team Village](#) - cont...(10:00-11:59 PDT) - [Evil Is Always a Bad Stylist: .NET Obfuscation with Roslyn](#) - Alexander Rodchenko,Ashley Hiram Muñoz,Eduardo Chavarro Ovalle
[Red Team Village](#) - [Living Off WebView2: Turning Microsoft's Browser into a Red Team Asset](#) - Murilo Caixeta
[Red Team Village](#) - [Commit, Push, Compromise: Attacking Modern GitHub Orgs](#) - Andrew Buchanan,Max CM
[Scambait Village](#) - cont...(10:00-15:59 PDT) - [Open Q&A](#) -
[Scambait Village](#) - cont...(10:00-15:59 PDT) - [KSCM Scambait Radio](#) -
[Scambait Village](#) - cont...(10:00-13:59 PDT) - [Scambait Bingo](#) -
[Social Engineering Community Village](#) - cont...(10:00-12:30 PDT) - [Social Engineering Community Village - Open Hours](#) -
[Social Engineering Community Village](#) - cont...(10:30-11:30 PDT) - [2027 SECVC Pre-Qualification Round - LIVE CALLS](#) -
[Social Engineering Community Village](#) - (11:30-12:30 PDT) - [Cold Calls](#) -
[Social Gatherings/Events](#) - cont...(09:00-11:59 PDT) - [Human Registration Open](#) -
[Social Gatherings/Events](#) - cont...(10:00-14:59 PDT) - [Music - SomaFM](#) -
[Social Gatherings/Events](#) - [Free Ham Radio License Exams](#) -
[Telecom Village](#) - cont...(10:20-13:59 PDT) - [Telecom Village CTF](#) - T-Mobile CTF Team
[The Diana Initiative](#) - [Threat Model your Career Workshop](#) - Chandan Vedavyas
[Voting Village](#) - cont...(10:00-13:59 PDT) - [Voting Village Lab](#) -

[Aerospace Village](#) - cont...(10:00-13:59 PDT) - [Mission: Compromised - Hacking a Satellite from the Ground Up](#) -
[Aerospace Village](#) - cont...(10:00-13:59 PDT) - [Drone Hacking Choose your Own Adventure](#) -
[Aerospace Village](#) - cont...(10:00-13:59 PDT) - [MOUSE Runner & Flappy Drone](#) -
[Aerospace Village](#) - cont...(10:00-13:59 PDT) - [Flight Simulator/EFB](#) -
[Aerospace Village](#) - cont...(10:00-13:59 PDT) - [Drone Hacking Workshop](#) -
[Aerospace Village](#) - cont...(10:00-13:59 PDT) - [SR-71 Blackbird Badge Challenge](#) -
[Aerospace Village](#) - cont...(10:00-13:59 PDT) - [Satellites Under Attack: Hands-On Satellite Security Threat Scenarios](#) -
[Aerospace Village](#) - cont...(10:00-13:59 PDT) - [Nebula Showdown: Space Systems Security CTF Adventure](#) -
[Aerospace Village](#) - cont...(10:00-13:59 PDT) - [SpaceCOP - Catch Me If You Can](#) -
[Aerospace Village](#) - cont...(10:00-13:59 PDT) - [Aviation ISAC Cybersecurity Challenge](#) -
[Aerospace Village](#) - cont...(10:00-13:59 PDT) - [Aerospace Ecosystem Resilience Innovation Environment \(AERIE\) Cyber Range](#) -
[Aerospace Village](#) - cont...(10:00-13:59 PDT) - [ARINC 664 CTF Challenge](#) -
[Aerospace Village](#) - cont...(10:00-13:59 PDT) - [DCNextGen - Space Grand Challenge - SatHack: The MOUSE-1 Mission](#) -
[Aerospace Village](#) - cont...(10:00-13:59 PDT) - [DCNextGen - RIC-1: ELT Localization Exercise - N3VR-G0N Down](#) -
[Aerospace Village](#) - cont...(10:00-13:59 PDT) - [DCNextGen - Bricks in the Air](#) -
[Aerospace Village](#) - cont...(10:00-13:59 PDT) - [Bricks in the Air](#) -
[AI Village](#) - cont...(10:00-13:59 PDT) - [AI Village: Village Open](#) -
[AI Village](#) - cont...(10:00-13:59 PDT) - [Cyber Mirage: Realtime Deepfake Demos](#) - Brandon Kovacs
[AI Village](#) - (12:30-12:59 PDT) - [AI Village: Closing Remarks](#) -
[AI Village](#) - [Pwning Agentic Browsers with PleaseFix: A New Vulnerability Class for 0-Click Takeover](#) - Stav Cohen
[AI Village](#) - (12:30-12:59 PDT) - [Leveraging Large Language Models for Policy, Regulatory, and Compliance in IoMT: Opportunities, Risks, and Safeguards](#) - Dr. Deepti Gupta,Sai Sitharaman
[AppSec Village](#) - cont...(11:30-12:30 PDT) - [search_vulns: Navigating the Fragmented Landscape of Vulnerability Data](#) - Dustin Born,Matthias Göhring
[AppSec Village](#) - (12:45-13:45 PDT) - [The Agent Asked. We Allowed. Now What?](#) - Liran Lavi,Sarit Yerushalmi
[AppSec Village](#) - cont...(10:15-12:59 PDT) - [Introduction to AI-Enhanced Threat Modeling Workshop](#) - Robert Hurlbut
[AppSec Village](#) - cont...(11:50-12:20 PDT) - [Finding Bugs Is Easy, Patching Isn't: Build Your Own Remediation Pipeline](#) - Mohan Kumar,Naveen
[AppSec Village](#) - cont...(11:00-12:59 PDT) - [Clash of Prompts: The World's First Prompt Battle Royale](#) - Darren McNelis,Jerome Roberts
[AppSec Village](#) - cont...(11:00-12:59 PDT) - [AppSec Quiz Gauntlet: Spot the Vulnerability](#) - Avek Kolech
[AppSec Village](#) - cont...(11:00-12:59 PDT) - [SBOM Find the Flaws](#) - Dmitry Raidman
[AppSec Village](#) - cont...(11:00-12:59 PDT) - [NPM Imposters - The malware detection card game](#) - Mackenzie
[Biohacking Village](#) - cont...(10:00-13:59 PDT) - [Embedded & Shredded: Advanced Embedded System Hacking](#) -
[Biohacking Village](#) - cont...(10:00-13:59 PDT) - [Biohacking Device Lab](#) -
[Blacks In Cyber Village](#) - [Monocultures Are Vulnerabilities: Representation and Security in STEM](#) - Ruben Stephen
[Bug Bounty Village](#) - [How We Built Xenoptic: A Walkthrough of Design, Infrastructure and Vulns!](#) - Adham Elmosalamy,Ahmed Attalla,Yousef Awad,Kasimir Schulz
[Call Center Village](#) - cont...(10:00-13:59 PDT) - [Call Center Village - Open](#) -
[Car Hacking Village](#) - cont...(10:00-13:59 PDT) - [Car Hacking Village Open](#) -
[Cloud Village](#) - cont...(11:00-12:59 PDT) - [The Autonomous Insider](#) - Naveen Reddy Pogalla,Hari Pranav Arun Kumar
[Cloud Village](#) - cont...(11:50-12:30 PDT) - [Foxveil: Cloud-Native Loader Tradecraft on Cloudflare, Netlify, and Discord](#) - Shani Kurtzberg,Zohar Buber
[Cloud Village](#) - (12:30-13:10 PDT) - [Root-as-a-Service: The Hidden Runtime of Azure AI Foundry](#) - Shani Peled
[CodeBloom](#) - [Game Time: Input, Output, and Variables](#) -
[Contests](#) - cont...(10:00-13:59 PDT) - [Code Cadaver: Break Every System. Save Your Friend.](#) -
[Contests](#) - [PWN UR H0M3 DDoS CTF Winner Announcements](#) -
[Contests](#) - cont...(10:00-12:59 PDT) - [CMD+CTRL Cyber Range: DarkMoney](#) -
[Contests](#) - cont...(10:00-13:59 PDT) - [AI Village - Hal CTF](#) -
[Contests](#) - cont...(10:00-13:59 PDT) - [AI Village Plays Pokemon: DEFCON Edition](#) - Nick Ashworth

[DCNextGen - A Teen BadgeMaker's Journey of Creation](#) - World Machine
[DEF CON Groups](#) - cont...(10:00-13:59 PDT) - [DEF CON Groups \(DCG\)](#) -
[DEF CON Talks](#) - [Your WAF Blocked Us, That Was The Exploit](#) - Remote Agent Takeover via Cloudflare, Sentry and Claude Zero-Day for data exfil - Barak Sternberg,Nevo Poran,Ron Bobrov
[DEF CON Talks](#) - [MSIX'd Up: Weaponizing the Modern Windows App Packaging Ecosystem](#) - Nick "zyn3rgy" Powers
[DEF CON Talks](#) - [1.1 Million Cameras, One Wildcard: Architectural Surveillance in an IoT Cloud](#) - Sammy Azdoufal
[DEF CON Talks](#) - cont...(11:30-12:30 PDT) - [BLE Theft Auto: How a Dealer-Installed Anti-Theft System Exposes Over a Million Cars to Theft](#) - Aaron Schulman,Jerry Yu,Yibo Wei
[DEF CON Talks](#) - (12:30-13:30 PDT) - [Chaining Microsoft Binaries to get Privileged Primitives in the Windows kernel](#) - Angelo Frasca Caccia
[DEF CON Talks](#) - cont...(11:30-12:30 PDT) - [From Fuzzer Noise to a Weaponized PHP Exploit: Exploiting a PHP Use-After-Free Vulnerability](#) - Can Oztas,Kağan Çapar
[DEF CON Talks](#) - (12:30-13:30 PDT) - [CUDA've done better - Hacking Nvidia GPUs for container-escape and privilege escalation](#) - Daniel "0xDACA" Cohen Hillel,Noam Trobishi
[DEF CON Training](#) - cont...(08:30-17:30 PDT) - [Blue vs Red Bootcamp: From Attacker Playbooks to Defender Detections](#) - Carlo Anez Mazurco,Mariana Ruiz
[DEF CON Training](#) - cont...(08:30-17:30 PDT) - [Influence Operations: Tactics, Defense, and Exploitation](#) - Greg Conti,Tom Cross
[DEF CON Training](#) - cont...(08:30-17:30 PDT) - [Full-Stack Pentesting Laboratory: 100% Hands-On + Lifetime LAB Access](#) - Dawid Czagan
[DEF CON Workshops](#) - cont...(09:00-12:59 PDT) - [Sold Out - Attacking Cloud APIs from the IoT Edge](#) - Rodney "BenevolentWorm" Beede
[DEF CON Workshops](#) - cont...(09:00-12:59 PDT) - [Sold Out - Building your own hardware hacking kit to Pentest Bluetooth, WIFI, and more.](#) - Dallas
[DEF CON Workshops](#) - cont...(09:00-12:59 PDT) - [Sold Out - Post-Quantum Cryptography \(PQC\) for Hackers](#) - Eric "Eijah" Anderson
[DEF CON Workshops](#) - cont...(09:00-12:59 PDT) - [Sold Out - Purple Protocol: Adversary emulation for everyone](#) - Patrick "PilotPat" Raiden,Ben "Marba\$" Strout,Brandon "D43m0n" Kraycirik
[DEF CON Workshops](#) - cont...(09:00-12:59 PDT) - [Sold Out - CI/CD Weaponization: Build It, Deploy It, Own It](#) - Ricardo Sanchez,Daniel Malvaceda
[DEF CON Workshops](#) - cont...(09:00-12:59 PDT) - [Sold Out - ICS Hack 'n Track](#) - Pedro Cabrera,Hannes "hercules_hannes" Heck,Sam Miorelli,Jordan Sanchez
[DEF CON Workshops](#) - cont...(09:00-12:59 PDT) - [Sold Out - Creating Shellcode for Hackers](#) - Bramwell "Bw3ll" Brizendine,Austin "quantumite" Norby,Micah Flack
[DEF CON Workshops](#) - cont...(09:00-12:59 PDT) - [Sold Out - Pivot, Hunt, Publish: An Offline, Hands-On CTI Workshop for Blue Teams and Threat Researchers](#) - Rushikesh Nandedkar
[Embedded Systems Village](#) - cont...(10:00-13:59 PDT) - [Exploit Bluetooth Low Energy with BLESPlloit and optional ESP32](#) - Slawomir Jasek
[Embedded Systems Village](#) - cont...(10:00-13:59 PDT) - [Embedded - 101 Labs](#) -
[Embedded Systems Village](#) - cont...(10:00-13:59 PDT) - [Embedded Systems Village CTF](#) -
[Game Hacking Village](#) - cont...(11:30-12:30 PDT) - [Yes, I froze an SNES for science](#) - dwangoAC
[Game Hacking Village](#) - (12:30-12:59 PDT) - [SH4ZAM: Accelerated Vector Math on the Sega Dreamcast](#) - Falco Girgis
[ICS Village](#) - [ThreatPatrol: Visualising the Modern Threat Landscape](#) - Viral Maniar
[ICS Village](#) - (12:30-12:59 PDT) - [Two NICs, Zero Trust: Pulling Apart a PAC Buried in Critical Infrastructure](#) - Adam Bromiley,Sam Thom
[IoT Village](#) - cont...(10:00-13:59 PDT) - [All About UART](#) -
[IoT Village](#) - cont...(10:00-13:59 PDT) - [Hands-On Hardware Hacking – From JTAG to Root, Memory Patching Boot Process for Root Access](#) -
[IoT Village](#) - cont...(10:00-13:59 PDT) - [Just Hacking Training](#) -
[IoT Village](#) - cont...(10:00-13:59 PDT) - [Cat-astrophic Hacking: Breaking Into Smart Litter Boxes](#) -
[IoT Village](#) - cont...(10:00-13:59 PDT) - [Raiders of the Lost Firmware: A Hands-On Workshop in IoT Firmware Archaeology](#) -
[IoT Village](#) - cont...(10:00-13:59 PDT) - [Smart Home in the Matter: Blink, Race, Attack CTF](#) -
[IoT Village](#) - cont...(10:00-13:59 PDT) - [Discover GE Appliances!](#) -
[IoT Village](#) - cont...(10:00-13:59 PDT) - [Expose Hidden Surveillance in Everyday Tech](#) -

IoT Village - cont...(11:00-13:30 PDT) - [Wi-Fi Self Defense & Hacker Hunting & For Beginners](#) - Kody Kinzie
 La Villa Community - [Red Robin: Don't Hack For Me, Hack With Me](#) - Juan Sequeira Piedra,Jose Urena
 Lonely Hackers Club - cont...(10:00-13:59 PDT) - [Lonely Hackers Club - Sticker Swap Table](#) -
 Lonely Hackers Club - cont...(10:00-13:59 PDT) - [Lonely Hackers Club - Lockpicking Table](#) -
 Lonely Hackers Club - [Lonely Hackers Club - CTF Winners Announcement](#) -
 Maker's Village - cont...(10:00-13:59 PDT) - [Makers' Village - Hacker Arts and Crafts](#) -
 Maker's Village - [Novice design in 3d space](#) - RedThorn
 Middle Easterns & Africans in Cyber Security (MEACS) - [The Dark Art of Alert Correlation: Extracting Attack Chains from Chaos](#) - Ezz Tahoun
 Middle Easterns & Africans in Cyber Security (MEACS) - [Where the Authorization Boundary Goes in Agent Workflows](#) - Mohamed Magdy AbuMuslim
 Misc - [Friendship Bracelets](#) -
 Mobile Hacking Community - cont...(10:00-13:59 PDT) - [Mobile Hacking Community - Open](#) -
 Noob Community - cont...(10:00-13:59 PDT) - [No Stupid Questions](#) -
 Noob Community - cont...(10:00-13:59 PDT) - [SANS Institute NetWars Labs](#) -
 Noob Community - cont...(10:00-13:59 PDT) - [Skillbit Labs](#) -
 Noob Community - cont...(10:00-13:59 PDT) - [TCM Security Labs](#) -
 Noob Community - cont...(10:00-13:59 PDT) - [Mentoring and Career Advice](#) -
 Noob Community - cont...(10:00-13:59 PDT) - [Kryptsec Labs](#) -
 Noob Community - cont...(10:00-13:59 PDT) - [Hack The Box DC Junior Ranger Program Challenge](#) -
 Noob Community - cont...(10:00-13:59 PDT) - [Arcanum Security Labs](#) -
 Noob Community - cont...(11:00-12:59 PDT) - [From Command Line to Center Stage: Hack Your Way to Confident Speaking](#) - James McQuiggan
 Noob Community - cont...(11:45-12:15 PDT) - [So You Want to Be a Red Teamer? The Reality Behind the Role](#) - Billy Giles
 Noob Community - (12:30-12:59 PDT) - [Be your own Agent: Career Journey and Advice from IT and STEM Educator to Cybersecurity Engineer](#) - Meghan Jacquot
 OSINT For Good Community - cont...(10:00-13:59 PDT) - [OSINT4Good Community - DC NextGen Content](#) -
 OSINT For Good Community - cont...(10:00-13:59 PDT) - [FINDX OSINT Educational Series](#) -
 OSINT For Good Community - cont...(11:30-12:45 PDT) - [Disaster Intelligence - The past, present, and future of situational awareness during a crisis](#) - Matt Green
 OSINT For Good Community - (12:15-12:45 PDT) - [Practical Privacy Defenses for the Paranoid](#) - Tina "Hek8te" Shakour
 OWASP Foundation - (12:30-12:59 PDT) - [Source of Truth: A Field Guide for Deep Technical Research](#) - Carley "51nk0r5w1m" Fant
 OWASP Foundation - cont...(10:30-12:30 PDT) - [2001: Agentic Odyssey in Threat Modeling](#) - Petra Vukmirovic
 OWASP Foundation - cont...(11:00-13:59 PDT) - [OWASP Chapter Meetup](#) -
 OWASP Foundation - [Let's Play! OWASP Cornucopia Threat Modeling](#) -
 Payment Village - [CAPTURE THE COIN - Announcement of the CTF Winners](#) -
 Physical Security Village - [Travel Security: Viewing Risks Through the Eyes of a Hacker](#) - Tim Roberts,Brent White
 Policy @ DEF CON - [Inference in the Infrastructure: Developing NIST AI RMF Resources for Resilient AI in Critical Systems](#) - Raymond Sheh,Martin Stanley
 Policy @ DEF CON - (12:30-13:59 PDT) - [Tactical Advocacy: Panel & Peer Sessions with EFF](#) - Thorin Klosowski,Cooper "Cybertiger" Quintin,Alexis Hancock,Cindy Cohn,Rory Mir
 Radio Frequency Village - cont...(10:00-13:59 PDT) - [Radio Frequency Village Events](#) -
 Radio Frequency Village - [RF CTF and World Wide War Drive Outbrief](#) - RF Hackers
 Recon Village - [Recon on Trial: The OSINT Operator's Legal Playbook](#) - David Cass
 Recon Village - (12:30-12:59 PDT) - [Building Hackbots](#) - Jason "jhaddix" Haddix
 Red Team Village - cont...(10:00-14:59 PDT) - [Attack Campaign in VR](#) - James Rice
 Red Team Village - [Do you feel in control? Analysis of AWS CloudControl API as an attack tool](#) - Bleon "gl4ssesbo1" Proko
 Red Team Village - [From Buffer Overflow to Blackout: Chaining Attacks Against Industrial Systems](#) - Fernando Mengali,Thiago Cunha da Silva
 Red Team Village - [The Air Is Hostile: RF Trust Assumptions in Modern Security Systems](#) - Mitch Breton
 Red Team Village - [Living Off the IDE: From Initial Access to Covert C2 in Modern AI Code Editors](#) - Edo Maland
 Red Team Village - [Agenthound: Mapping Multi-Hop Credential Chains Across MCP, A2A, and LLM Gateways](#) - Adithyan Arun Kumar
 Red Team Village - [Breaking and Defending NEURO: Hands-On AI Stack Attack CTF with Cisco Secure AI](#) - Jason Ludwig

[Scambait Village](#) - cont...(10:00-15:59 PDT) - [Open Q&A](#) -
[Scambait Village](#) - cont...(10:00-15:59 PDT) - [KSCM Scambait Radio](#) -
[Scambait Village](#) - cont...(10:00-13:59 PDT) - [Scambait Bingo](#) -
[Social Engineering Community Village](#) - cont...(10:00-12:30 PDT) - [Social Engineering Community Village - Open Hours](#) -
[Social Engineering Community Village](#) - cont...(11:30-12:30 PDT) - [Cold Calls](#) -
[Social Gatherings/Events](#) - cont...(10:00-14:59 PDT) - [Music - SomaFM](#) -
[Social Gatherings/Events](#) - [Friends of Bill W](#) -
[Social Gatherings/Events](#) - cont...(11:00-12:59 PDT) - [Free Ham Radio License Exams](#) -
[Telecom Village](#) - cont...(10:20-13:59 PDT) - [Telecom Village CTF](#) - [T-Mobile CTF Team](#)
[The Diana Initiative](#) - (12:17-13:16 PDT) - [Quiet Room](#) -
[The Diana Initiative](#) - cont...(11:00-12:59 PDT) - [Threat Model your Career Workshop](#) - Chandan Vedavyas
[Voting Village](#) - cont...(10:00-13:59 PDT) - [Voting Village Lab](#) -

[Aerospace Village](#) - cont...(10:00-13:59 PDT) - [SpaceCOP - Catch Me If You Can](#) -
[Aerospace Village](#) - cont...(10:00-13:59 PDT) - [SR-71 Blackbird Badge Challenge](#) -
[Aerospace Village](#) - cont...(10:00-13:59 PDT) - [Nebula Showdown: Space Systems Security CTF Adventure](#) -
[Aerospace Village](#) - cont...(10:00-13:59 PDT) - [Satellites Under Attack: Hands-On Satellite Security Threat Scenarios](#) -
[Aerospace Village](#) - cont...(10:00-13:59 PDT) - [Mission: Compromised - Hacking a Satellite from the Ground Up](#) -
[Aerospace Village](#) - cont...(10:00-13:59 PDT) - [Drone Hacking Choose your Own Adventure](#) -
[Aerospace Village](#) - cont...(10:00-13:59 PDT) - [MOUSE Runner & Flappy Drone](#) -
[Aerospace Village](#) - cont...(10:00-13:59 PDT) - [Flight Simulator/EFB](#) -
[Aerospace Village](#) - cont...(10:00-13:59 PDT) - [Drone Hacking Workshop](#) -
[Aerospace Village](#) - cont...(10:00-13:59 PDT) - [Aerospace Ecosystem Resilience Innovation Environment \(AERIE\) Cyber Range](#) -
[Aerospace Village](#) - cont...(10:00-13:59 PDT) - [Aviation ISAC Cybersecurity Challenge](#) -
[Aerospace Village](#) - cont...(10:00-13:59 PDT) - [ARINC 664 CTF Challenge](#) -
[Aerospace Village](#) - cont...(10:00-13:59 PDT) - [DCNextGen - Space Grand Challenge](#) - [SatHack: The MOUSE-1 Mission](#) -
[Aerospace Village](#) - cont...(10:00-13:59 PDT) - [DCNextGen - RIC-1: ELT Localization Exercise](#) - [N3VR-G0N Down](#) -
[Aerospace Village](#) - cont...(10:00-13:59 PDT) - [DCNextGen - Bricks in the Air](#) -
[Aerospace Village](#) - cont...(10:00-13:59 PDT) - [Bricks in the Air](#) -
[AI Village](#) - cont...(10:00-13:59 PDT) - [AI Village: Village Open](#) -
[AI Village](#) - cont...(10:00-13:59 PDT) - [Cyber Mirage: Realtime Deepfake Demos](#) - Brandon Kovacs
[AppSec Village](#) - cont...(12:45-13:45 PDT) - [The Agent Asked. We Allowed. Now What?](#) - Liran Lavi, Sarit Yerushalmi
[Biohacking Village](#) - cont...(10:00-13:59 PDT) - [Embedded & Shredded: Advanced Embedded System Hacking](#) -
[Biohacking Village](#) - cont...(10:00-13:59 PDT) - [Biohacking Device Lab](#) -
[Blacks In Cyber Village](#) - [DeNISTifying Technology: Paradigm Shifting To Quantum Encryption, Post Cryptography, and Digital Forensics](#) - Aisha Berry
[Bug Bounty Village](#) - (13:45-14:15 PDT) - [Bug Bounty Village Closing Ceremony](#) - Bug Bounty Village Staff
[Call Center Village](#) - cont...(10:00-13:59 PDT) - [Call Center Village - Open](#) -
[Car Hacking Village](#) - cont...(10:00-13:59 PDT) - [Car Hacking Village Open](#) -
[Cloud Village](#) - cont...(12:30-13:10 PDT) - [Root-as-a-Service: The Hidden Runtime of Azure AI Foundry](#) - Shani Peled
[Cloud Village - Closing Talk](#) - Jayesh Singh Chauhan
[CodeBloom](#) - [What is AI?](#) - Sam Mosley
[Contests](#) - cont...(10:00-13:59 PDT) - [Code Cadaver: Break Every System. Save Your Friend.](#) -
[Contests](#) - cont...(10:00-13:59 PDT) - [AI Village - Hal CTF](#) -
[Contests](#) - cont...(10:00-13:59 PDT) - [AI Village Plays Pokemon: DEFCON Edition](#) - Nick Ashworth
[Contests](#) - [Bug Bounty Village CTF Awards](#) - Bug Bounty Village Staff
[DCNextGen](#) - (13:30-14:30 PDT) - [DCNextGen Closing Ceremonies](#) - BiaSciLab
[DEF CON Groups](#) - cont...(10:00-13:59 PDT) - [DEF CON Groups \(DCG\)](#) -
[DEF CON Talks](#) - (13:30-14:59 PDT) - [Contest Closing Ceremonies & Awards](#) -
[DEF CON Talks](#) - [Chaining Logical Bugs for Reliable Windows LPE](#) - Bocheng "Crispr" Xiang, HeeChan "heegong123" Kim
[DEF CON Talks](#) - cont...(12:30-13:30 PDT) - [Chaining Microsoft Binaries to get Privileged Primitives in the Windows kernel](#) - Angelo Frasca Caccia
[DEF CON Talks](#) - (13:30-14:30 PDT) - [Witchcraft Solver: Automated 0day Discovery in Stripped Binaries](#) - Jonathan "endrazine" Brossard
[DEF CON Talks](#) - cont...(12:30-13:30 PDT) - [CUDA've done better - Hacking Nvidia GPUs for container-escape and privilege escalation](#) - Daniel "0xDACA" Cohen Hillel, Noam Trobishi
[DEF CON Talks](#) - (13:30-13:59 PDT) - [Taking on the Dark Fleet... in Cyberspace!](#) - Kenneth Miltenberger, Shane Cancilla
[DEF CON Training](#) - cont...(08:30-17:30 PDT) - [Blue vs Red Bootcamp: From Attacker Playbooks to Defender Detections](#) - Carlo Anez Mazurco, Mariana Ruiz
[DEF CON Training](#) - cont...(08:30-17:30 PDT) - [Influence Operations: Tactics, Defense, and Exploitation](#) - Greg Conti, Tom Cross
[DEF CON Training](#) - cont...(08:30-17:30 PDT) - [Full-Stack Pentesting Laboratory: 100% Hands-On + Lifetime LAB Access](#) - Dawid Czagan

[Embedded Systems Village](#) - cont...(10:00-13:59 PDT) - [Exploit Bluetooth Low Energy with BLESPlloit and optional ESP32](#) - Slawomir Jasek
[Embedded Systems Village](#) - cont...(10:00-13:59 PDT) - [Embedded - 101 Labs](#) -
[Embedded Systems Village](#) - cont...(10:00-13:59 PDT) - [Embedded Systems Village CTF](#) -
[IoT Village](#) - cont...(10:00-13:59 PDT) - [All About UART](#) -
[IoT Village](#) - cont...(10:00-13:59 PDT) - [Just Hacking Training](#) -
[IoT Village](#) - cont...(10:00-13:59 PDT) - [Raiders of the Lost Firmware: A Hands-On Workshop in IoT Firmware Archaeology](#) -
[IoT Village](#) - cont...(10:00-13:59 PDT) - [Hands-On Hardware Hacking – From JTAG to Root, Memory Patching Boot Process for Root Access](#) -
[IoT Village](#) - cont...(10:00-13:59 PDT) - [Cat-astrophic Hacking: Breaking Into Smart Litter Boxes](#) -
[IoT Village](#) - cont...(10:00-13:59 PDT) - [Smart Home in the Matter: Blink, Race, Attack CTF](#) -
[IoT Village](#) - cont...(10:00-13:59 PDT) - [Expose Hidden Surveillance in Everyday Tech](#) -
[IoT Village](#) - cont...(10:00-13:59 PDT) - [Discover GE Appliances!](#) -
[IoT Village](#) - cont...(11:00-13:30 PDT) - [Wi-Fi Self Defense & Hacker Hunting & For Beginners](#) - Kody Kinzie
[La Villa Community](#) - [La Villa - Closing Ceremony \(ESP\)](#) -
[Lockpick Village](#) - [Intro to Lockpicking](#) -
[Lonely Hackers Club](#) - cont...(10:00-13:59 PDT) - [Lonely Hackers Club - Sticker Swap Table](#) -
[Lonely Hackers Club](#) - cont...(10:00-13:59 PDT) - [Lonely Hackers Club - Lockpicking Table](#) -
[Maker's Village](#) - cont...(10:00-13:59 PDT) - [Makers' Village - Hacker Arts and Crafts](#) -
[Maker's Village](#) - (13:30-13:59 PDT) - [Visable Mending, repair and reinforce](#) -
[Middle Easterns & Africans in Cyber Security \(MEACS\)](#) - [MEACS Trivia, Games and Networking](#) -
[Mobile Hacking Community](#) - cont...(10:00-13:59 PDT) - [Mobile Hacking Community - Open](#) -
[Nix Vegas Community](#) - [Nix Vegas Closing Ceremony](#) -
[Nix Vegas Community](#) - (13:30-14:30 PDT) - [Unconference](#) -
[Noob Community](#) - cont...(10:00-13:59 PDT) - [Mentoring and Career Advice](#) -
[Noob Community](#) - cont...(10:00-13:59 PDT) - [Kryptsec Labs](#) -
[Noob Community](#) - cont...(10:00-13:59 PDT) - [Hack The Box DC Junior Ranger Program Challenge](#) -
[Noob Community](#) - cont...(10:00-13:59 PDT) - [Arcanum Security Labs](#) -
[Noob Community](#) - cont...(10:00-13:59 PDT) - [SANS Institute NetWars Labs](#) -
[Noob Community](#) - cont...(10:00-13:59 PDT) - [Skillbit Labs](#) -
[Noob Community](#) - cont...(10:00-13:59 PDT) - [No Stupid Questions](#) -
[Noob Community](#) - cont...(10:00-13:59 PDT) - [TCM Security Labs](#) -
[Noob Community](#) - [Noob Community - Conference Closing](#) -
[OSINT For Good Community](#) - cont...(10:00-13:59 PDT) - [F1NDX OSINT Educational Series](#) -
[OSINT For Good Community](#) - cont...(10:00-13:59 PDT) - [OSINT4Good Community - DC NextGen Content](#) -
[OSINT For Good Community](#) - [Building a Student-Led OSINT Program to Investigate Cryptocurrency Fraud](#) - Angela Ramos
[OWASP Foundation](#) - cont...(11:00-13:59 PDT) - [OWASP Chapter Meetup](#) -
[Policy @ DEF CON](#) - cont...(12:30-13:59 PDT) - [Tactical Advocacy: Panel & Peer Sessions with EFF](#) - Thorin Klosowski,Cooper "Cybertiger" Quintin,Alexis Hancock,Cindy Cohn,Rory Mir
[Radio Frequency Village](#) - cont...(10:00-13:59 PDT) - [Radio Frequency Village Events](#) -
[Red Team Village](#) - cont...(10:00-14:59 PDT) - [Attack Campaign in VR](#) - James Rice
[Red Team Village](#) - cont...(12:00-13:59 PDT) - [Do you feel in control? Analysis of AWS CloudControl API as an attack tool](#) - Bleon "gl4ssesbo1" Proko
[Red Team Village](#) - cont...(12:00-13:59 PDT) - [From Buffer Overflow to Blackout: Chaining Attacks Against Industrial Systems](#) - Fernando Mengali,Thiago Cunha da Silva
[Red Team Village](#) - cont...(12:00-13:59 PDT) - [The Air Is Hostile: RF Trust Assumptions in Modern Security Systems](#) - Mitch Breton
[Red Team Village](#) - cont...(12:00-13:59 PDT) - [Living Off the IDE: From Initial Access to Covert C2 in Modern AI Code Editors](#) - Edo Maland
[Red Team Village](#) - [M0us3: A Lightweight, Multi Session C2 Framework with a Rust based Windows Implant](#) - Aryan Jogia
[Red Team Village](#) - [Hacking the Human-in-the-Loop](#) - Alexander "Zombie",Lee McWhorter
[Scambait Village](#) - cont...(10:00-15:59 PDT) - [Open Q&A](#) -
[Scambait Village](#) - cont...(10:00-15:59 PDT) - [KSCM Scambait Radio](#) -
[Scambait Village](#) - cont...(10:00-13:59 PDT) - [Scambait Bingo](#) -

[Social Gatherings/Events](#) - cont...(10:00-14:59 PDT) - [Music](#) - [SomaFM](#) -
[Telecom Village](#) - cont...(10:20-13:59 PDT) - [Telecom Village CTF](#) - [T-Mobile CTF Team](#)
[The Diana Initiative](#) - cont...(12:17-13:16 PDT) - [Quiet Room](#) -
[The Diana Initiative](#) - [The Diana Initiative](#) - [Open time](#) -
[Voting Village](#) - cont...(10:00-13:59 PDT) - [Voting Village Lab](#) -

[Return to Index](#) - [Locations Legend](#)

[Bug Bounty Village](#) - cont...(13:45-14:15 PDT) - [Bug Bounty Village Closing Ceremony](#) - Bug Bounty Village Staff
[CodeBloom](#) - [Work Session: Ciphers](#) -
[DCNextGen](#) - cont...(13:30-14:30 PDT) - [DCNextGen Closing Ceremonies](#) - BiaSciLab
[DEF CON Talks](#) - cont...(13:30-14:59 PDT) - [Contest Closing Ceremonies & Awards](#) -
[DEF CON Talks](#) - [Hacking Jetskis - from Sea-Don't to Sea-Doo](#) - stacksmashing
[DEF CON Talks](#) - cont...(13:30-14:30 PDT) - [Witchcraft Solver: Automated 0day Discovery in Stripped Binaries](#) - Jonathan "endrazine" Brossard
[DEF CON Talks](#) - [Talkers Without Borders: Worldwide Free Speech without an Internet Connection](#) - T. Gwyddon "data" Owen,amp
[DEF CON Training](#) - cont...(08:30-17:30 PDT) - [Blue vs Red Bootcamp: From Attacker Playbooks to Defender Detections](#) - Carlo Anez Mazurco,Mariana Ruiz
[DEF CON Training](#) - cont...(08:30-17:30 PDT) - [Influence Operations: Tactics, Defense, and Exploitation](#) - Greg Conti,Tom Cross
[DEF CON Training](#) - cont...(08:30-17:30 PDT) - [Full-Stack Pentesting Laboratory: 100% Hands-On + Lifetime LAB Access](#) - Dawid Czagan
[Nix Vegas Community](#) - cont...(13:30-14:30 PDT) - [Unconference](#) -
[Noob Community](#) - cont...(13:05-15:55 PDT) - [Noob Community - Conference Closing](#) -
[Red Team Village](#) - cont...(10:00-14:59 PDT) - [Attack Campaign in VR](#) - James Rice
[Red Team Village](#) - [beacon injected with HOOKCHAIN 2026](#) - Arnold Jared Morales Yopez
[Red Team Village](#) - [Ghost in the Water: Simulating a Nation-State PLC Sabotage Campaign](#) - Blessen Thomas,Javier Hernández,Wojciech Poparda
[Red Team Village](#) - [DFMI: Weaponizing MSI Installers for Fileless Code Execution](#) - Anıl Çelik
[Scambait Village](#) - cont...(10:00-15:59 PDT) - [KSCM Scambait Radio](#) -
[Scambait Village](#) - cont...(10:00-15:59 PDT) - [Open Q&A](#) -
[Social Gatherings/Events](#) - cont...(10:00-14:59 PDT) - [Music](#) - SomaFM -
[Telecom Village](#) - [Telecom Village CTF Awards Ceremony](#) -

Sunday - 15:00 PDT

[Return to Index](#) - [Locations Legend](#)

[DEF CON Talks](#) - [DEF CON Closing Ceremonies & Awards](#) - [Jeff "The Dark Tangent" Moss](#)

[DEF CON Training](#) - cont...(08:30-17:30 PDT) - [Blue vs Red Bootcamp: From Attacker Playbooks to Defender Detections](#) - [Carlo Anez Mazurco](#),[Mariana Ruiz](#)

[DEF CON Training](#) - cont...(08:30-17:30 PDT) - [Influence Operations: Tactics, Defense, and Exploitation](#) - [Greg Conti](#),[Tom Cross](#)

[DEF CON Training](#) - cont...(08:30-17:30 PDT) - [Full-Stack Pentesting Laboratory: 100% Hands-On + Lifetime LAB Access](#) - [Dawid Czagan](#)

[Noob Community](#) - cont...(13:05-15:55 PDT) - [Noob Community](#) - [Conference Closing](#) -

[Scambait Village](#) - cont...(10:00-15:59 PDT) - [KSCM Scambait Radio](#) -

[Scambait Village](#) - cont...(10:00-15:59 PDT) - [Open Q&A](#) -

[Return to Index](#) - [Locations Legend](#)

[DEF CON Talks](#) - cont...(15:00-17:30 PDT) - [DEF CON Closing Ceremonies & Awards](#) - Jeff "The Dark Tangent" Moss

[DEF CON Training](#) - cont...(08:30-17:30 PDT) - [Blue vs Red Bootcamp: From Attacker Playbooks to Defender Detections](#) - Carlo Anez Mazurco, Mariana Ruiz

[DEF CON Training](#) - cont...(08:30-17:30 PDT) - [Influence Operations: Tactics, Defense, and Exploitation](#) - Greg Conti, Tom Cross

[DEF CON Training](#) - cont...(08:30-17:30 PDT) - [Full-Stack Pentesting Laboratory: 100% Hands-On + Lifetime LAB Access](#) - Dawid Czagan

[Return to Index](#) - [Locations Legend](#)

[DEF CON Talks](#) - cont...(15:00-17:30 PDT) - [DEF CON Closing Ceremonies & Awards](#) - Jeff "The Dark Tangent" Moss

[DEF CON Training](#) - cont...(08:30-17:30 PDT) - [Blue vs Red Bootcamp: From Attacker Playbooks to Defender Detections](#) - Carlo Anez Mazurco, Mariana Ruiz

[DEF CON Training](#) - cont...(08:30-17:30 PDT) - [Influence Operations: Tactics, Defense, and Exploitation](#) - Greg Conti, Tom Cross

[DEF CON Training](#) - cont...(08:30-17:30 PDT) - [Full-Stack Pentesting Laboratory: 100% Hands-On + Lifetime LAB Access](#) - Dawid Czagan

Sunday - 22:00 PDT

[Return to Index](#) - [Locations Legend](#)

[Social Gatherings/Events](#) - (22:30-01:59 PDT) - [DEF CON After party @ LIV Fontainebleau](#) -

Speaker List

Albert (4n6h4x0r)
01dbae
Overkilll
Overkilll
0xHera
0xHera
Infocalypse
4ng3lhacker
Aamiruddin Syed
Aamiruddin Syed
Aarav Juneja
Aaron "Ironical" Rosenmund
Aaron Crow
Aaron Guzman
Aaron Honeycutt
Aaron Kaiser
Aaron Kaiser
Aaron Schulman
Aaron Tulino
Aaron Wasserman
Aaron Wasserman
Abbie Gonzalez (pronounced AB)
Abhay Bhargav
Abhay Bhargav
Abhijeet Kumar
Abhijeet Kumar
Abhijith "Abx" B R
Abhijith "Abx" B R
Abhijith "Abx" B R
Abhinav "TweetsFromPanda" Pandagale
Abhinav Khanna
Abhinav Khanna
Abhinav Singh
Abhinav Singh
Abhinav Verma
Abhinav Verma
Abhinav Verma
Abhishek J M
Abhishek J M
Abraham Aranguren
Abraham Aranguren
Abraxas3d
Ac0rn
Adam "w00tock" Toscher
Adam "w00tock" Toscher
Adam Batori
Adam Bromiley
Adam Bromiley
Adam Hickey
Adam Pennington
Adam Shostack

Adham Elmosalamy
Adithyan Arun Kumar
Aditi Narasimhan
Ads Dawson
Ads Dawson
Ads Dawson
Advait Patel
Adventures of Illya
Adventures of Illya
AfterGlow
Ahmed Attalla
Ahmed Nagi Nasr
Ahmeen Muhammad
Ahmet Furkan Aydogan
Ahmet Furkan Aydogan
Aidan "luu176" Nakache
Aidan Quimby
Aisha Berry
Aiswarya Venkitesh
Akanksha Raghvesh
Akbar "0xsensei" Abdullayev
Akbar "0xsensei" Abdullayev
Akib Sayyed
Akira Nishikawa
Akira Nishikawa
Albert "yz9yt" Corzo
Albin Vattakattu
Alchemmer
Alchemmer
Alchemmer
Alcyon Junior
Alec Summers
Alejandro "Oxedh" Hernando
Alejandro Vázquez Vázquez
Alek Amrani
Aleksandr Krasnov
Alessandra Rizzo
Alethe Denis
alevsk
Alex Brumen
Alex Decious
Alex Hurtado
Alex Plaskett
Alex Radocea
Alex Tipan
Alexander "Zombie"
Alexander Rodchenko
Alexander Wren
Alexandrine Torrents
Alexandrine Torrents
Alexandru Uifalv
Alexis Hancock
Alexis Hancock
Ali "logic-breaker" Kabeel

Allie Zagrodnik
Allie
Allison Gallo
AltF4
AltF4
AltKey
Alyssa Coley
Aman Rawat
Amanda Kollmorgan
Amber Bennoui
Amber Bennoui
Amber Bennoui
Amber Bennoui
Amber Bennoui
Amin Hussien
Amir Zaltzman
Amit Sharma
amp
Amy McMahon
Anant Shrivastava
Anant Shrivastava
Anant Shrivastava
Anant Shrivastava
Anant Shrivastava
Anant Shrivastava
Anant Shrivastava
Andra Lezza
André Cirne
André Cirne
Andrea Brosio
Andrea Brosio
Andrea Brosio
Andreas Kaltsounis
Andrés Restrepo
Andres Sabas
Andrew 'bunnie' Huang
Andrew Bellini
Andrew Buchanan
Andrew Case
Andrew Griess
Andrew Hendela
Andrew Krug
Andrew Lebedinsky
Andrew Ohnstad - N3OCQ
Andrew Quill
Andrew Rioux
Andrew Tierney
Andrzej Olchawa
Andrzej Olchawa
Andy Dennis
Andy Dennis
Andy Dennis
Andy Dennis
Andy Hendrickson
Andy Hull

Angela "BlondeTechie" Ramos
Angela Ramos
Angela Ramos
Angela Ramos
Angelo Frasca Caccia
Anil Celik
Anil Celik
Aniruddha Biyani
Anirudh Anand
Anirudh Anand
Anirudh Pratap Singh
Anissa Elias
Anita Ding
Anita Ding
Anıl Çelik
Ankit Vashisth
Ankit Vashisth
Anne Drago
Anne Marie Schumann
Annie Meaney
Anshu Gupta
Anthony "Coin" Rose
Anthony "Coin" Rose
Anthony "Coin" Rose
Anthony "Coin" Rose
Anthony "Coin" Rose
Anthony Hendricks
Anthony Johnson
Anthony Russell
Anthony Russell
Anup Swamy Veena
Anurag Swarnim Yadav
Anurag Swarnim Yadav
Apoorwa Joshi
Aravind Sreekanth Pallavoor
Arcanum Information Security Team
Archwisp
Ariana Mirian
Arie Haenel
Ariel "arl_rose" Garcia
Ariel Ropek
Arielle Baine
Arif
Arity0
Arity0
Ariz Soriano
Ariz Soriano
Ariz Soriano
Arjun "Peper" Suresh
Arjun "Peper" Suresh
Arjun "Peper" Suresh
Armaan Pathan
Armend Gashi
Armend Gashi
Arnaud SOULLIE

Arnaud SOULLIE
Arnav Garg
Arnold Jared Morales Yepez
Arnold Jared Morales Yepez
Arnold Jared Morales Yepez
Arnold Jared Morales Yepez
Arnold Wey
Arun Nair
Arun Nair
Arvind Singh
Arvind Singh
Arvind Singh
Aryan Jogia
Asher Davila
Asher Davila
Asher Davila
Ashley Hiram Muñoz
Ashley Hiram Muñoz
Ashley Hiram Muñoz
Ashley S
Ashley Sequeira
Assaf Morag
Atsushi Sada
Atsushi Sada
Aumkareshwar DS
Aumkareshwar DS
Austin "quantumite" Norby
Austin Sturm
Avek Kolech
Avek Kolech
Avek Kolech
Avek Kolech
Avinash Majeti
Avinash Majeti
Avinash Majeti
Avishai Efrat
Aviv Donenfeld
Ayaan Qayyum
Ayaan Qayyum
Ayan Islam
Bar Kaduri
Barak Sternberg
Barbara Simons
Barno Kaharova
Beau Woods
Ben "Marba\$" Strout
Ben "NahamSec" Sadeghipour
Ben "NahamSec" Sadeghipour
Ben "NahamSec" Sadeghipour
Ben "The Cyber Sensei" Crenshaw
Ben Flatgard
Ben Gardiner
Ben Higgins
Benito "paperclipsvinny" Saucedo
Bianca C. Ionescu/reconcerto

Bianca C. Ionescu/reconcerto
BiaSciLab
BiaSciLab
Bill "hevnsnt" Swearingen
Bill Graydon
Bill Reyor
Bill Reyor
Bill Reyor
Billy Giles
Billy Giles
Billy Giles
Birgitte Jordal
Bleon "gl4ssesbo1" Proko
Bleon "gl4ssesbo1" Proko
Blessen Thomas
Blessen Thomas
Bo-Shiun "bronson113" Yen
Bobby Graydon
Bocheng "Crispr" Xiang
Bogdan "BOTEZATU"
Bogdan Steele
Borja "borjmz" Martinez
Brad "Sno0ose" Ammerman
Bradán Lane
Braelynn Luedtke
Bramwell "Bw3ll" Brizendine
Brandon "D43m0n" Kraycirik
Brandon Bailey
Brandon Kovacs
Brandon Kovacs
Brandon Kovacs
Brandon
Brandy Smith
Brandy Smith
Brent Louie
Brent Louie
Brent Louie
Brent White
Brett Alexander Tolbert
Brett Tolbert
Brian Baskin
Brian Brushwood
Brian Brushwood
Brian Brushwood
Brian Burnett
Brian DeMuth
Brian DeMuth
Brian G. Rodiles Delgado
Britt Kemp
Bruce Schneier
Bruce Schneier
Bruce Schneier
Bruce Schneier
Bruno Mendes
Bryan

Bryant Pickford
Bryson Bort
Buddha
Buddha
Buddha
Bug Bounty Village Staff
Bug Bounty Village Staff
Buğrahan Yücel
Buğrahan Yücel
C\$
cale "calebot" smith
Can Kurnaz
Can Oztas
Can Oztas
Cannibal
Carley "51nk0r5w1m" Fant
Carlo Anez Mazurco
Carlo Anez Mazurco
Carlo Anez Mazurco
Carlo Anez Mazurco
Carlo Anez Mazurco
Carlo Anez Mazurco
Carlo Meijer
Carlota Bindner
Carmela Gonzales
Carmeshia Miller
Carole House
Carsten Schürmann
Cassandra (muteki) Young
Cassandra (muteki) Young
Catherine Cassell
cdC & Veilid crew
Champ
Chandan Vedavyas
Chandru J
Charel "1C0nur3r" Morris
Charel "1C0nur3r" Morris
Charles Grow
Chase Phelps
Chelsea Button
Chen Doytshman
Chen Doytshman
Cheryl Biswas
Chiao-Lin Yu "Steven Meow"
Chirag "3xpl01tc0d3r" Savla
Chirag "3xpl01tc0d3r" Savla
Chirag "3xpl01tc0d3r" Savla
Chirag Savla
Chris "dafinga" Maenner
Chris "dafinga" Maenner
Chris "flyingtoasters" Holt
Chris Claunch
Chris Connelly
Chris Haller
Chris Kulakowski

Chris Navarrete
Chris Navarrete
Chris Painter
Chris Ryan
Chris Ryan
Chriss Hansen
Christian "DeadlyFluVirus" Nuss
Christian Dameff
Christian Nicholson
Christiane Borges Santos
Christina Parry
Christine Billingsley
Christine Von Raesfeld
Christopher "repermunky" Aziz
Christopher "TRIODE" Le
Christopher "xoreaxeaxeax" Domas
Christopher DeCarmen
Christopher DeCarmen
Christopher Hernandez
Christopher Hernandez
Chrysostomos Manousis
Ciarán "monke" Cotter
Cindy Cohn
Cindy Cohn
Cindy Cohn
Cindy Cohn
Cindy Cohn
Cindy Cohn
Clara Davis
Clayton Boozell
Cliff "GritsnGravy" Friedel
Cliff Neve
Cliff Stoll
Cloud Village
CoD_Segfault
Cody Spooner
Colonel Panic
Cong Zhang
Cooper "Cybertiger" Quintin
Cooper "Cybertiger" Quintin
Corey Ball
Courtney McCarty
Cøry "interpunkt" Solovewicz
CPV Gold Bug Team 2026
Craig "jafo" Buchanan
Curt Barnard
Cynthia Ardman
D3adA55
Daemon Chadeau
Dallas
Dalton Cox
Dan Borgogno
Dan Borgogno
Dan Borgogno
Dan Gansel

Dan Goga
Dan Niefeld
Dan W0BDP Norte
Dana Pirvu
Dane Sherrets
Daniel "0xDACA" Cohen Hillel
Daniel "Daniboy" França Lima
Daniel Baker
Daniel Baker
Daniel Bravo
Daniel Cuthbert
Daniel Fabien
Daniel Genkin
Daniel Goldberg
Daniel Isler
Daniel Justice
Daniel Koranek
Daniel Koranek
Daniel Malvaceda
Daniel Monzon
Danielle Eason
Danilo Erazo
Danny Quist
Darcy "@Drc3p0" Neal
Darren McDonald
Darren McNelis
Darren Meyer
Dave "Rebelcadet" Ortiz
David "0xdf" Forsythe
David "davidrxchester" Rochester
David C Eight
David Case
David Cass
David Collins
David Fiser
David J. Castillo-Cornejo
David Jefferson
David Jefferson
David McDonald
David Nathans
David Rushmer
Davidson Mizael
Dawid Czagan
Dawid Czagan
Dawid Czagan
Dawid Czagan
Dean Macris
Deanna Heon
Deanna Heon
Delta Blue
Dennis Giese
Deral Heiland
Derek C.
Desnos Anthony
Devin Lynch

Dhiraj Mishra
Dhiyaneshwaran Balasubramaniam
Dhruva Goyal
Diego "rehrrar" Salazar
Diego Cotel
Diego Staino
Dillon Lee
Dimple Gajra
Dinmukhammed "Celestial" Kabiden
Diptendu Kar
DJ Scythe
DJ XORAC
Dmitry Raidman
Dmitry Raidman
Dmitry Raidman
Dmitry Raidman
Dmitry Raidman
Do Truong Giang "FSNaix"
Dolev Taler
DolphinVG
Dominika Pietrzak
Don Bogert
Doron Kapah
dotornot
Doug Mooney
Douglas W. Jones
Dr. Allan Friedman
Dr. Deepti Gupta
Dr. Fatou Sankare
Dr. Fatou Sankare
Dr. Hassan Karim
Dr. Katrina Rosseini
Dr. Louis DeWeaver III
Dr. Nina Kollars
Dr. Nina Kollars
Dr. Tia Pope
Dr. Wanda T. Jones-Heath
Dr. Xavier-Lewis Palmer
Dr. Zulfikar Ramzan
Drew Kirkpatrick
Drew Springall
Drew Thompson
Dual Core
Duncan Buell
Dustin "ph1r3574r73r" Farley
Dustin Born
Dustin
dwangoAC
Dylan Gururajan
Eddie Miro
Eden Yardeni
Edna Jonsson
Edo Maland
Eduardo Chavarro Ovalle
Eduardo Chavarro Ovalle

Eduardo Contreras
Edward Morris
EFF
Efim Boieru
Efim Boieru
Ege Feyzioglu
Elad Meged
Elad Meged
Eleonora Losiouk
Eli Shparaga
Eli Woodward
Eli Woodward
Eli Woodward
Elizabeth Biddlecome
Elizabeth Eigner
Elizabeth Eigner
Elizabeth Rasnick
Elzer Pineda
Elzer Pineda
Elzer Pineda
Emanuel Gawrieh
Emile "TheSytten" Fugulin
Emilie Jørstad
Emily "@astradotpng" Astranova
Emma Latuszek
Emma Yuan Fang
Emma Yuan Fang
Eric "Eijah" Anderson
Eric Escobar
Eric Escobar
Eric Labrador
Erica Rachel Andrews
Erik Alcantara
Erika Lee
Erwin Karincic (Dollarhyde)
Ethan Carter Edwards
Ethan Carter Edwards
Eunji choi
Evan Anderson
Evan Cook
Evan
Evolve Security Academy
Evolve Security Academy
Ezra Woods
Ezz Tahoun
Ezz Tahoun
Ezz Tahoun
Ezz Tahoun
Ezz Tahoun
Ezz Tahoun
Ezz Tahoun
Fabien Guillebot
Fae Blu3Bird" Carlisle
Fagan Afandiyev
Falco Girgis

Farid Zakaria
Farid Zakaria
Farzaan Kaiyom
Fede Pacheco
Federico Kirschbaum
Felipe Solferini
Fernando Mengali
Fernando Mengali
Filipi Pires
Filipi Pires
Filipi Pires
Filipi Pires
Florian Schweins
Florian Schweins
fr4vian
Francesco Costa
Francesco La Spina
Frank Victory
Fred Heiding
Freddy Martinez
Freeman Slaughter
Fukusuke Takahashi
Fukusuke Takahashi
Furkan Fatih Demir
Gabriel Gegenhuber
Gal Bar Nahum
Gannon "Dorf" Gebauer
Gannon "Dorf" Gebauer
Garrett Freibott
Garrett Freibott
Garrett Gee
Garrett Gee
Gaston Aznarez
Gavin Zhong
Gavin Zhong
Geoff Hale
Geoff Hale
Geoff Sweet
George Scheibe
Georgia Weidman
Georgia Weidman
Gerardo Mejia
Giacomo "GiacLenzo2109" Lenzini
Gibson
Gigi Xiaoqing Liu
Gigi Xiaoqing Liu
Gigi Xiaoqing Liu
Gijs Rijnders
Gil Weizman
Gilgamesh
Glendon Chong
Gordon Long
Gowthamaraj Rajendran
Gowthamaraj Rajendran
Grant Versfeld

Greg Albrecht
Greg Albrecht
Greg Anderson
Greg Conti
Greg Conti
Greg Conti
Greg Conti
Greg Goldberg
Gregory "lumberhack" Disney-Leugers
Guanxing Wen
Gwendal Mognier
Gwendal Mognier
HackeMate
Haley Ring
Hallvard Nygard
Hamspiced
hamster
Hana Christensen
Hana Christensen
Hanley Shun
Hannah L
Hannah L
Hannes "hercules_hannes" Heck
Hari Pranav Arun Kumar
Harsha Potu
Hassan Mohamad
HD "hdm" Moore
Heather Adkins
Heather West
HeeChan "heegong123" Kim
Heidi Potter
Heiner García
Helen Oakley
Helen Oakley
Helen Oakley
Hemanth Gorijala
Hemanth Gorijala
Henry Danielson Hankashyyk
hikae
hikae
Horacio Bazán
Hrvoje Mišetić
Hugo van den Toorn
HUI Kwun Tai
hunny
hunny
hunny
hunny
Hxr1
HyunJun "Beaver King" Kwon
HyunJun "Beaver King" Kwon
Iain Jackson
Iain Jackson
ialleejy

ialleejy
Ian Harris
Ian Roos
Ibai Castells
Iceman
Icetre Normal
iDigitalFlame
Iggy
Ignacio Navarro
Inga Cherny
InsiderPHD
Inti "securinti" De Ceukelaire
Irvin Lemus
Isabel Manjarrez
Isabel Manjarrez
Isabel Manjarrez
Isabella "4ng3lhacker" Barnett
Itay Saraf
Izdihar
J Fridley
Jack Cable
Jack Rhysider
Jacob Gutierrez
Jacob Wall
Jad Meouchy
Jad Meouchy
Jae Sung Kim
Jai Kumar Sharma
Jai Kumar Sharma
Jake "Hubbl3" Krasnov
Jake "Hubbl3" Krasnov
Jake "Hubbl3" Krasnov
Jake Braun
Jake Braun
Jalen Chuang
James "Acorn221" Arnott
James "albinowax" Kettle
James Bowie
James Campbell
James Hawk
James McQuiggan
James Rice
James Sheppard
James Sheppard
James Stanger
James Utley PhD
James Williams
James(GSMA)
Jamie Hill-Daniel
Janakiram Meka
Janet Vertesi
Janet Vertesi
Janet Vertesi
Jared "GonePhishing402" Graff
Jared "GonePhishing402" Graff

Jared Dobbelaer
Jared Dygert
Jared Stroud
Jared
Jaron Bradley
Jarrod Rizer
Jason "jhaddix" Haddix
Jason "jhaddix" Haddix
Jason "jhaddix" Haddix
Jason "jhaddix" Haddix
Jason "jhaddix" Haddix
Jason "jhaddix" Haddix
Jason Clinton
Jason Ludwig
Jason Odoom
Jason Strange
Jason Veara
Jason Vogt
Jason Wareham
Javier Bernardo
Javier Hernández
Javier Hernández
Jayesh Singh Chauhan
Jayesh Singh Chauhan
Jayson E. Street
Jayson E. Street
JB
JC
JC
JD D
JDT
Jeff "r3plicat" Tully
Jeff "The Dark Tangent" Moss
Jeff "The Dark Tangent" Moss
Jeff "The Dark Tangent" Moss
Jeff "UltraSunshine" G
Jeff Crume
Jeff Daniels
Jeff Daniels
Jeff Foley
Jeff Foley
Jeff Moss
Jeff Rothblum
Jeff Rothblum
Jenko "edleft" Hwong
Jenko "edleft" Hwong
Jenn Gile
Jenn
Jennifer Granick
Jennifer Slaybaugh
Jennifer VanAntwerp
Jeremy Banker - K0JLB
Jeremy Banker - K0JLB
Jeremy Banker - K0JLB
Jeremy Schiefer

Jerome Roberts
Jerry Yu
Jess Hoffman
Jesse Michael
Ji'an "azraelxumo" Zhou
Jianjia Yu
Jianjia Yu
Jie Wu
Jigar Bhavsar
Jim Manico
Jim Manico
Jiří Vinopal
Jiří Vinopal
Jiwoon Yoo
Joanna -
João Maria Campos Donato
João Pedro Tricta
Joe "jbohack"
Joe "SecurelyFitz" FitzPatrick
Joe Folk
Joe Slowik
Joe Uchill
Joey Melo
Joey Melo
Johann "wunderwuzzi23" Rehberger
John "clearbluejar" McIntosh
John "clearbluejar" McIntosh
John "clearbluejar" McIntosh
John "clearbluejar" McIntosh
John Banghart
John Banghart
John Kotheimer
John McCary
John O'Connor
John Odum
Jon "C4V3M4N" Milkins
Jon "flakpaket" Gorenflo
Jon "GainSec" Gaines
Jon Marler (K4CHN)
Jon Marler (K4CHN)
Jon McCoy
Jon Rhodes
Jonathan "endrazine" Brossard
Jonathan Coradi
Jonathan Xue
Jordan Bonagura
Jordan Sanchez
Jorge Acevedo Canabal
Jorge Acevedo Canabal
Jorge Braniff
Jos Wetzels
Jos Wetzels
Jose Rivas
Jose Rivas
Jose Rivas

Jose Urena
Josep Albors
Josep Albors
Joseph Long
Joseph Wilson
Joseph Wilson
Josh Benaloah
Joshua Marpet
Joshua Morgan
Juan Camilo Palacio Arango
Juan Martinez Blanco
Juan Martinez Blanco
Juan Sequeira Piedra
Juan Urbano Stordeur
Juan Urbano Stordeur
Julia Kucharska
Julian Zottl
Julie Brunias
Juno
Justin Dray
K Singh
K0YTL
Kağan Çapar
Kai Glauber
Kainu ~
Kaitlyn Handelman
Kamel Ghali
Kamel Ghali
Kameron "clovismint" Bettridge
Kamil Szczurowski
Kangwon Lee
Karan Dwivedi
Karan Sajjani
Karen Ng
Karol Piekarski
Karol Piekarski
Karol Piekarski
Kasimir Schulz
Katharina "Kat S" Sommer
Katherine Pratt
Katie Fejer
Katie Paxton-Fear
Katie Paxton-Fear
Katie Trimble-Noble
Kayrene Woods
Keanu "RedByte" Nys
Keith Hoodlet
Ken Gannon /
Ken Johnson
Ken Johnson
Ken Munroe
Ken Pyle
Kendall Spencer
Kendall Spencer
Kendall Spencer

Kenechukwu Nwodo
Kennashka DeSilva
Kenneth "kenleejl" Lee
Kenneth "kenleejl" Lee
Kenneth Miltenberger
Kenny J
Kenny J
Kenny J
Kenyatta Thomas
Keren Elazari
Kevin "kdrwins" Dela Rosa
Kevin "kdrwins" Dela Rosa
Kevin Buck
Kevin Colley
Kevin Shelley
Kevin
Khael Kugler
KL4R10N
Klaus Wunder
Kody Kinzie
Kody Kinzie
Kody Kinzie
Kody Kinzie
Kody Kinzie
Kody Kinzie
Kolja Grassmann
Kolja Grassmann
Konrad Jędrzejczyk
Konrad Jędrzejczyk
Konstantinos Karagiannis
Korstiaan Stam
Korstiaan Stam
Kotaro "@Decamark / @BinaryPoodle" Osugi
Krishna Chaganti
Krishna Chaganti
Kristen Sanders
Kristian Karlsen
Krity Kharbanda
Krity
Kumar Ashwin
Kurt Opsahl
kvprashant
Kyle Barboza
Kyle Dickinson
Kyle Hubbard
Kyle Quest
Kyler McElroy
Kyler McElroy
Kyprianos "kavasilo" Vasilopoulos
Kyul
Kyul
La Alsulaim
LambdaCalculus
LambdaCalculus
Landon Rice

Langston Clement
Larry Pesce
Laura Scherling
Laura Scherling
Lawton Pittenger
Leandro Cuzzo
Lee McWhorter
Lee McWhorter
Lei "Ilfamsec" Lu
Leigh Gilbert
Leigh Gilbert
Leigh Gilbert
Leigh-Anne Galloway
Lenin Alevski
Lenin Alevski
Lenin Alevski
Lenin Alevski
Leron Gray
Leslie Gutschow
Lester Godsey
Levi Schuck
Levone Campbell
Levone Campbell
Lidan
Lillian Ash Baker
Lindsey Cerkovnik
Lindsey Cerkovnik
Lindsey Cerkovnik
Liran Lavi
Lisa Olsen
Lisandro Ubiedo
Liz Wharton
Logan MacLaren
Lozaning
Luca Borzacchiello
Luis Pazmino
Lukas Stefanko
Luke Cycon
Luke Szramowski
M-Nelly
M-Nelly
M-Nelly
m0nkeydrag0n
M41w4r3
Mackenzie Jackson
Mackenzie Jackson
Mackenzie
Mackenzie
Mackenzie
Mackenzie
Mackenzie
Madeline Sedgwick
Madhu Akula
Madhu Akula
Madison Ficorelli

Magen Wu
Makoto "Mr.Rabbit" Sugita
Makoto "Mr.Rabbit" Sugita
Maksim Kuskov
Malachi Walker
Malav Vyas
Manbir Gulati
Marcelle Lee
Marcia Hofmann
Marcie Wise
Marcin Dudek
Marco A. Alanis Komiyama
Marcos "h3xduck" Bajo
Marek Zmysłowski
Marek Zmysłowski
Mariana Ruiz
Mariana Ruiz
Mariana Ruiz
Mariana Ruiz
Marie Moe
Marilyn Marks
Mario Lobo
Mario Lobo
Marios Gyftos
Mark Foudy
Mark Gaddy
Mark Trumbour
Mark Vaitsman
Marshall Livingston
Martin "MasorX" Strohmeier
Martin Stanley
Martin Vigo
Martzen Haagsma
Mathias Detmers
Matias Armándola
Matt Blaze
Matt Blaze
Matt Blaze
Matt Blaze
Matt Burch
Matt Burch
Matt Caldwell
Matt Gaffney
Matt Galligan
Matt Green
Matt Green
Matteo Giordano
Matthew O'Reilly
Matthew Wein
Matthias Göhring
Matthias Göhring
mattrix
Maureese Williams
Maurice Turner
Mauro Eldritch

Mauro Eldritch
Mauro Eldritch
Mauro Eldritch
Max vonBlankenburg
Max A
Max CM
Max Springer
max
Maximilian Guenther
Maya Parizer
McKay Hardy
medus4
medus4
medus4
Medus4
Megan Squire
Megg Sage
Meghan Jacquot
Mehdi Ziazi
Mehmet Önder Key
Mehmet Önder Key
Mehmet Önder Key
Mehmet Önder Key
Mehmet Önder Key
Meitar Ronen
Metehan Arslan
Micah Flack
Michael "MsvB" Schloh
Michael "v3ga" Aguilar
Michael "v3ga" Aguilar
Michael “sparky” Moore
Michael Brennan
Michael Cardwell
Michael Chan
Michael Flynn
Michael Glass
Michael Glass
Michael Kim
Michael Leibowitz
Michael Lenz
Michael Moore
Michael Moore
Michael Ortiz
Michael Ortiz
Michael Reimsbach
Michael Reimsbach
Michael Reimsbach
Michael Reimsbach
Michael Rivera
Michael Skelton
Michael Skelton
Michael Specter
Michael Specter
Michael Sulmeyer
Michal Kamensky

Mickey "@HackingThings" Shkatov
Miguel Fernandez
Mike "Chicolinux" Guirao
Mike "TakSec" Takahashi
Mike Holcomb
Mike Lisi
Mike Manrod
Mikhail Ilin
Miranda Tedholm
Mishaal Khan
Miss Jackalope
Mitch Breton
Mitch Herckis
MLP
MLP
MLP
Mohamed AbuMuslim
Mohamed Magdy AbuMuslim
Mohammed Ilyas Ahmed
Mohan Kumar
Monish Alur Gowdru
Monnappa K A
Monnappa K A
Morgan Jones
Morton Schenk
Moses Frost
Moshe Berntsein
MrBill
Mudita Khurana
Mukesh Aggarwal
Mukesh Aggarwal
Murilo Caixeta
Muskan Tomar
Muthu Kumar
Muzzammil Mohammed
Muzzammil Mohammed
mx
N A
N3rd H3Rder
Nadine Farid Johnson
Nancy Brainerd
Naomi Brockwell
Narmina Karimova
Narmina Karimova
Nataly "someone_somewhere"
Natan Morette
Natan Morette
Nate Moore
Nate Moore
Nate Young
Nathan Keys
Nathan Sawyer
Nathan Sawyer
Naveen Reddy Pogalla
Naveen

Nefeli Georgilas
Neha Gautam
Neha Gautam
Nelson Colon
Nelson Rafael Colón Merán
Nelson Rafael Colón Merán
Nevo Poran
Nicholas "gouldnicholas" Gould
Nicholas DeMeo
Nicholas Miazzo
Nick "7urb01" Copi
Nick "zyn3rgy" Powers
Nick Ashworth
Nick Ashworth
Nick Ashworth
Nick
Nick
Nico Dekens
Nikita Kronenberg
Nikkia Henderson
Nikos "nickvourd" Vourdas
Nikos "nickvourd" Vourdas
Nikos "nickvourd" Vourdas
Niranjanaa Ragupathy
Nishant Tayade
Nishith Sinha
Nishith Sinha
Nitay Bachrach
Noam Trobishi
Numaan Huq
Nuno Rodrigues Carvalho
Nur "BurritoTheNurrito" Gucu
Nur "BurritoTheNurrito" Gucu
Nur Gucu
Nykolas Muldrow
nyx
Ofek Itach
Ohm-I
Olaf Hartong
Oleksandr Mirosh
Oliveira Junior
Omescan ~
Omescan ~
Omer Farooq
Omer Farooq
Omer Farooq
Omri "beta_b0t" Ben Bassat
Ozgun "ozzy" Kultekin
Ozgun "ozzy" Kultekin
Ø1
Pamela 'Pam' Feld
Pankaj Sontakke
Pankaj Sontakke
Parag Kalay
Parag Kalay

Param "P7R7M"
Param "P7R7M"
Pardhiv Reddy
Pardhiv Reddy
PatAttack
Patricia Vargas Leon
Patrick "gigstorm" Kiley
Patrick "PilotPat" Raiden
Patrick Sliney
Patrick Smyth
Patrick Smyth
Patrick Smyth
Patrick Smyth
Patrick Walsh
Patrick Wardle
Patrick Wardle
Paul Goffar
Paul Nakasone
Pavan "pavanreddysec" Reddy
Pedro "drop" Paniago
Pedro Cabrera
Pedro Fortuna
Petra Vukmirovic
Peyton "p80n-sec" Kennedy
Phil Englert
Philip "AlephNull" Werlau
Philip Acosta
Philip Stark
Philip Stark
Philip Stark
Philippe "pilvar" Dourassov
Piero "p33_p33_" Picasso
Pierre "Abyss Watcher" Breton
Piffd0s
polybius
pradameinhof
Preston Zen
Pujita Sahni
Qiqing Huang
RabidMoosery
RADM John Mauger
Radu Stefan Voloaga
Rafa "bane" Gutierrez
Rafael Castilho Silva
Rafael Felix
Rafael Felix
Rahul Saranjame
Rahul Saranjame
Ram "n2r"
Ranganatha Rao Sridhar
Ranganatha Rao Sridhar
Raphael "rcss" Silva
Raunak "Trouble1" Parmar
Raunak "Trouble1" Parmar
Raunak "Trouble1" Parmar

Raunak "Trouble1" Parmar
Rayden Chia
Raymond Sheh
Razvan Gavrilă
Razvan Gavrilă
Rebecah Miller
Rebekah Brown
Red Team Alliance
Red Team Alliance
Redon Gashi
Redon Gashi
redshiftzero
RedThorn
Reino Mostert
RELAY
RemoteNemesis
RemoteNemesis
RF Hackers
RF Hackers
RF Hackers
Ricardo Fradique
Ricardo Fradique
Ricardo Loura
Ricardo Sanchez
Richard DeMillo
Richard Shmel
Richard Shmel
Ricky (0xpsilocyber) Banda
Rico Komenda
RinoaPoison
Rishi "rxerium" C
Rishi "rxerium" C
Rishi "rxerium" C
Rishi Kant
Rishi Kant
Rithvik Vibhu
Rithwik "the131" Jayasimha
Ritvik "RoYalGamr" Goyal
Ritvik Arya
Riyaz Walikar
Riyaz Walikar
Robbie Galfrin
Robert "ProXy" Kruczek
Robert "pwcraek" Weiss
Robert "pwcraek" Weiss
Robert "zizkill" Shala
Robert Herrera
Robert Hurlbut
Robert Pafford
Robert Pimentel
Robert Pimentel
Robin
Rod Soto
Rod Soto
Rodney "BenevolentWorm" Beede

Rodrigo "Sp0oKeR" Montoro
Roe Idan
Roey Ben Chaim
Roger "arma" Dingledine
Roger Egan
Rohan Vazarkar
Rohini
Roman Bohuk
Romel "r0r0x" Marin
Ron Ben Yizhak
Ron Ben Yizhak
Ron Bobrov
Ronald Broberg
Ronald Broberg
Rory Mir
Ruben Gonzalez
Ruben Gonzalez
Ruben Stephen
Ruchik Dave
Rudy Mendoza
Rudy Mendoza
Rudy Ristich
Rushikesh Nandedkar
Ryan "@rj_chap" Chapman
Ryan "@rj_chap" Chapman
Ryan "BadAt_Computers" Bonner
Ryan "Hackgnar" Holeman
Ryan "Nightlark" Mast
Ryan "Nightlark" Mast
Ryan "ryancbarnett" Barnett
Ryan Bonner
Ryan Bonner
Ryan Bonner
Ryan Hausknecht
Ryan Macias
Ryan Montgomery
Ryan Murray
Ryan Nolette
Ryan Zagrodnik
Ryan Zmuda
Saad Nasir
Saar Pearl
Sachin "sachinnthakuri" Thakuri
Sadhana Sainarayanan
Sadiq "Sdqmd"
Sahan Fernando
Sai Sathvik Ruppa
Sai Sathvik Ruppa
Sai Sitharaman
Sai Vernekar
saikishu
saikishu
Sajan Shetty
Sajan Shetty
Saksham Agrawal

Saksham Agrawal
Saksham Agrawal
Sam Bowne
Sam Jadali
Sam Miorelli
Sam Mosley
Sam Mosley
Sam Mosley
Sam Mosley
Sam Mosley
Sam Mosley
Sam Thom
Samanta Aranda
Samantha Pearlstein
Samantha Pearlstein
Samantha Pearlstein
Samantha Pearlstein
Samantha Schwartz
Samet Berk Simsek
Samet Berk Simsek
Samet Can Tasci
Samet Can Tasci
Sammy Azdoufal
Samson Adewale
Samuel B. G.
Samuel B. G.
Samuel B. G.
Samuel B. G.
Samuil Nikolov
Sana Talwar
Sandeep "pyro" Jayashankar
Sandra Stibbards
Sanjeev Sharma
Santiago Sepúlveda Veliz
Sara "testingSoul" Martinez
Sara "testingSoul" Martinez
Sarah "scba" Miller
Sarah Hume
Sarah Muriel
Sarah Muriel
Sarah
Sarit Yerushalmi
Sarthak Taneja
Sarthak Taneja
Scotch and Bubbles
Scott Shackelford
Scott Thompson
Scott Weston
Sean McConoughey
securient
Seedon D'Souza
Seeyew Mo
Selim Jaafar
Selma Jenker

Sercan Okur
Sercan Okur
Seth Art
Seth Benning
Seth Benning
Seth Law
Seth Law
Shad Brown
Shahak Morag
Shai Laron
Shane Cancilla
Shane Young
Shane Young
Shani Kurtzberg
Shani Peled
Shasheen Bhandodkar
Shavvon "TheSiren" Cintron
Shayan Alinejad
Shemeka Chance Jeffrey
Sherry Michael
Shlomie "shlibness" Liberow
Shreya G Savadatti
Shrimant Subhash More
Siddharth Kumar
Silas Cutler
Simcha Kosman
Simcha Kosman
Simon Correa
Simon Maxwell-Stewart
Simone Bossi
Sindhura Kona
Sitaraman Subramanian
Siva Sareddu
Sk!tz0
Sk!tz0
Skittish & Bus
Slawomir Jasek
Slawomir Jasek
Slawomir Jasek
Slawomir Jasek
Smriti Gaba
Smriti Gaba
Smriti Gaba
Snow
Sohail Saha
some-natalie
Spencer Alessi
stacksmashing
Stanislav Dashevskyi
Stav Cohen
Stav Cohen
Stepan Konicek
Stephanie Doyle
Stephanie Doyle
Stephanie

Stephen Glombicki
Stephen Hilt
Stephen Richter
Stephen Schneider
Steven "Stengo" Ngo
Steven Flores
Subho Halder
Sunil Yadav
Suriya Prasath S
Suzanne Borders
Suzanne Borders
Sven Schleier
Sven Schleier
Sven Schleier
Sydney "letswastetime" Marrone
Sydney "letswastetime" Marrone
Sydney Johns
Syntax + Luna
Szymon Skalski
Szymon Skalski
T-Mobile CTF Team
T-Mobile CTF Team
T-Mobile CTF Team
T-Mobile CTF Team
T. Gwyddon "data" Owen
TaeWoo Kim
Tahseen Rabbani
Tal Peleg
Tamil Mathi T.
Tamir Yehuda
Tanishq Rupaal
Tanishq Rupaal
Tanya "SheHacksPurple" Janca
Tanya "SheHacksPurple" Janca
Tati
Tatiana U
Taylor Roberts
TBD
Teazee
Teazee
Teazee
Ted Harrington
Temel Demir
Temel Demir
Temel Demir
The Hacking Games
The HRV Contest Team
The Wrew
TheGibson
Thiago Cunha da Silva
Thomas Mason
Thomas Roccia
Thomas Wilhelm
Thorin Klosowski
Tiffany Scheurenbrand

Tim Doerges
Tim Doerges
Tim Harper
Tim Roberts
Timothy E. Bates
Tina "Hek8te" Shakour
Tobia "mastersplinter" Righi
Tobias Diehl
Tobias Diehl
Todd Fletcher
Tokugero
Tom "t0xodile" Stacey
Tom Cross
Tom Cross
Tom Cross
Tom Cross
Tom McCarthy
Tom VanNorman
Toni de la Fuente
Tony Lee
Tony Martin-Vegue
Tony Martin
Tony Turner
Tori Noble
Trace Labs Staff
Travis Berent
Trevor Flynn
Trevor Timm
TRIODE
Tristan Ross
Tristan Ross
Tyrone E. Wilson
Uğur "uJohn" Can ATASOY
Uğur "uJohn" Can ATASOY
Uriel Kosayev
Vangelis Stykas
VanHelen
Venkata Jayaram Yalla
Venkata Jayaram Yalla
Venky Raju
Venky Raju
Veronica Kovah
Victor Gomez
Victoria Keeler
Victoria Keeler
Vijay Anand
Vikramaditya Narayan
Vince "bitpusher" Weppner
Vincent "Vinnybod" Rose
Vincent "Vinnybod" Rose
Vincent "Vinnybod" Rose
Vincent Sloan
Vincent Sloan
Vinitha Mathiyazhagan
Vinod Shrimali

Vinod Shrimali
Vipul Ujawane
Viral Maniar
Vishnu Prasad
Vishnu Prasad
Vitaly Simonovich
Vitor "busf4ctor" Falcao Habibe Costa
Vitor "busf4ctor" Falcao Habibe Costa
Vivek Ponnada
Vladimir "G1ND1L4" Tokarev
Vladimir "G1ND1L4" Tokarev
Vladimir "G1ND1L4" Tokarev
W. Martín Villalba
W. Martín Villalba
W. Martín Villalba
wasabi
Wayne Williams
Weihan Goh
Wes Miller
Wes Thurner
Wes Wagstaff
Wesley McGrew
Wesley McGrew
Whit Taylor
Will Alexander
Will Hatzer
Will McCardell
Will McCardell
Will Thomas
Will Thomas
Will Thomas
William Gates
William Liu
William Reyor
Willie Zhang
Wojciech Poparda
Wojciech Poparda
World Machine
Wouter Bokslag
Wouter Bokslag
Wouter Bokslag
Xavier "@xaferima" Riofrio Machado
Xeno Kovah
Xia Hua
Xia Hua
Xingyu Wang
XtraRaj
Yaara Shriki
Yael Grauer
Yang Liu
Yaniv "PSYMAG" Menasherov
Yannick LaRue
Yannick LaRue
Yannick LaRue
Yannick LaRue

Yariv Tal
Yariv Tal
Yasmin Eady
Yehyeong Lee
Yekaterina Shevchenko
Yevhen Pervushyn
Yi Ting Shen
Yianna Paris
Yianna Paris
Yibo Wei
Yll "0xBabar0ka" Berisha
Yll "0xBabar0ka" Berisha
Yoann "OtterHacker" DEQUEKER
Yoann "OtterHacker" DEQUEKER
Yoshihito Adachi
Yotam Perkal
Young Seuk Kim
Yousef Awad
Yu Terada
Yuval Hanoach Hirschenbein Sadde
Zach Mathis
Zach Mathis
Zack Allen
zeta
Zeus "LightningGod" Chan
Zeus "LightningGod" Chan
Zhassulan "cocomelonc" Zhussupov
Zhassulan "cocomelonc" Zhussupov
ZhengChao Wen
Zhenghan Wang
Zhengyu Liu
Zhengyu Liu
Zibran Sayyed
Zibran Sayyed
ZipZapZop
Zoe Reid+Echo419
Zoe
Zohar Buber
Zoziel Freire
; Oscar Skjerven

Talk List

?Cube - Contests
?Cube - Contests
?Cube - Contests
.edu Community Mixer - .EDU Community
"Can it Ham" Antenna Testing - Ham Radio Village
"Trust Us, It's Secure": Why Internet Voting Isn't - Voting Village
[Virtual] National Service Panel - CTU,BIC,MCPA - Blacks In Cyber Village
+61: the Australian Embassy - Social Gatherings/Events
\$750 and a Weekend: Passive Direction Finding Across the Spectrum with KrakenSDR - Radio Frequency Village
\$unLight Sh4d0w5 - Contests
\$unLight Sh4d0w5 - Contests
\$unLight Sh4d0w5 - Contests
0-Day Hunting Table: Come Join the Vulnpocalypse - Red Team Village
1.1 Million Cameras, One Wildcard: Architectural Surveillance in an IoT Cloud - DEF CON Talks
10 years of K-rad (Hackers.Town Party) - Social Gatherings/Events
15th Cycleoverride Bike Ride at DEF CON - Social Gatherings/Events
2001: Agentic Odyssey in Threat Modeling - OWASP Foundation
2026 is the New 2016: Relearning the Lessons from the "Year of the Data Breach" - Crypto & Privacy Village
2027 SECVC Pre-Qualification Round - LIVE CALLS - Social Engineering Community Village
2027 SECVC Pre-Qualification Round - Social Engineering Community Village
2nd Annual Spades Night & Uno Tournament - Social Gatherings/Events
3d Designing basics, 5 minute prints in Tinkercad - Maker's Village
3D Printing: Data, Discretion, and Design - DCNextGen
5N4CK3Y - Contests
5N4CK3Y - Contests
5N4CK3Y - Contests
6 years of Adversary Village! Keeping up with the adversaries and why it takes a village - Adversary Village
8 Out of 10 Banks in Belgium HATE This One Weird eID RCE - DEF CON Talks
a [REDACTED] history of this hobby - Bug Bounty Village
A 5G Digital Twin CTF for Hacking Carrier-Grade Infrastructure - Telecom Village
A 5G Digital Twin CTF for Hacking Carrier-Grade Infrastructure - Telecom Village
A Billion-User Blast Radius: Owning ChatGPT's Secure Sandbox - AppSec Village
A Billion-User Blast Radius: Owning ChatGPT's Secure Sandbox - AI Village
A Droidwork Orange: A Longitudinal Study of Android Security Research - Mobile Hacking Community
A Framework for Evaluating AI-Enabled Social Engineering - Social Engineering Community Village
A hands-on hour with IDA: reverse-engineer a real DLL-sideload attack from safe, purpose-built samples. No experience required — you'll crack your first binary in the first ten minutes. - Malware Village
A New Hope for SSRF: Exploiting Credential Relay from APIM to AI Foundry - Cloud Village
A Provider for the MOFia - Distributed Post-Ex Capabilities - DEF CON Talks
A Real-Time Battle with a Card-Testing Adversary - Payment Village
A Teen BadgeMaker's Journey of Creation - DCNextGen
AC Scanner: The Post-Quantum Cryptographic Exposure and CBOM Generator. You Need This! - Demo Labs
AC Scanner: The Post-Quantum Cryptographic Exposure and CBOM Generator. You Need This! - Demo Labs
Ace/Aro Meetup - Queercon Community
AD-Necromancer: Resurrecting Forgotten Control Paths in Active Directory - Demo Labs
AD-Necromancer: Resurrecting Forgotten Control Paths in Active Directory - Demo Labs
Advanced Cloud Incident Response in Azure and Microsoft 365 - DEF CON Training
Advanced Cloud Incident Response in Azure and Microsoft 365 - DEF CON Training
Advanced Topics in LoRa Meshes - Ham Radio Village
Advanced Windows Binary Exploitation - DEF CON Training
Advanced Windows Binary Exploitation - DEF CON Training
Adversarial Thinking: The Art of Dangerous Ideas - DEF CON Training

Adversarial Thinking: The Art of Dangerous Ideas - DEF CON Training
Adversary Village Tour - The Diana Initiative
Aegis of the Vulnerable: A Unified Pipeline for AI-Based SAST - AppSec Village
Aerospace Cybersecurity Student Research Spotlight: Cal Poly - Aerospace Village
Aerospace Cybersecurity Student Research Spotlight: ERAU - Aerospace Village
Aerospace Ecosystem Resilience Innovation Environment (AERIE) Cyber Range - Aerospace Village
Aerospace Ecosystem Resilience Innovation Environment (AERIE) Cyber Range - Aerospace Village
Aerospace Ecosystem Resilience Innovation Environment (AERIE) Cyber Range - Aerospace Village
Aerospace Village Tour - The Diana Initiative
AgentBreaker: A blind spot detector for your coding agents - AI Village
Agenthound: Mapping Multi-Hop Credential Chains Across MCP, A2A, and LLM Gateways - Red Team Village
Agentic AI Supply chain Vulnerability lab - Red Team Village
Agentic AppSec: Harnessing LLMs - DEF CON Training
Agentic AppSec: Harnessing LLMs - DEF CON Training
Agentic Chaos - What 86K+ Agent Codebases Reveal About 700K+ Exposed AI Systems - AppSec Village
Agentic RE: Automating Reverse Engineering & Vulnerability Research with AI - DEF CON Training
Agentic RE: Automating Reverse Engineering & Vulnerability Research with AI - DEF CON Training
Agents & Exploits: Hacking OWASP VWAD - OWASP Foundation
Agents of Chaos: A Field Guide to How Agentic AI Gets Owned, and What Trust Nothing Looks Like in Practice - Middle Easterns & Africans in Cyber Security (MEACS)
Agents on Alert: Building an AI-Powered Threat Investigation Framework - Blacks In Cyber Village
AI + SOC 101 Bootcamp: Building Modern Security Operation Skills with AI Integration - DEF CON Training
AI + SOC 101 Bootcamp: Building Modern Security Operation Skills with AI Integration - DEF CON Training
AI Agent Security Masterclass: Attacking and Defending Autonomous AI Systems - DEF CON Training
AI Agent Security Masterclass: Attacking and Defending Autonomous AI Systems - DEF CON Training
AI and You: Staying Safe in the AI Era - DCNextGen
AI Art Battle - Contests
AI Cuts Both Ways: Using AI to Find More Bugs, and Finding the New Bugs AI Creates - Bug Bounty Village
AI finds and writes my Android exploits now - Mobile Hacking Community
AI for Defenders 101 - Blue Team Village
AI Hacking for Noobs - Noob Community
AI Hacking Workshop: Bug Bounty Edition - Bug Bounty Village
AI Nightmare: Hacking at 0-Hour - Bug Bounty Village
AI Pentesting is not a Vibe Check - OWASP Foundation
AI Pentesting Trivia Showdown - AppSec Village
AI Pentesting Trivia Showdown - AppSec Village
AI Pentesting Trivia Showdown - AppSec Village
AI Pentesting Trivia Showdown - AppSec Village
AI Pipeline for N-days Weaponization - Demo Labs
AI Pipeline for N-days Weaponization - Demo Labs
AI Safety Theater: What the RAISE Act Regulates — and What It Does Not - Policy @ DEF CON
AI SecureOps: Attacking & Defending AI Applications & Agents - DEF CON Training
AI SecureOps: Attacking & Defending AI Applications & Agents - DEF CON Training
AI Security: Hype, Hacks, and the Future of Defense - Blue Team Village
AI Village - Hal CTF - Contests
AI Village - Hal CTF - Contests
AI Village - Hal CTF - Contests
AI Village Plays Pokemon: DEFCON Edition - Contests
AI Village Plays Pokemon: DEFCON Edition - Contests
AI Village Plays Pokemon: DEFCON Edition - Contests
AI Village Tour - The Diana Initiative
AI Village: Closing Remarks - AI Village
AI Village: Opening Remarks - AI Village
AI Village: Village Open - AI Village
AI Village: Village Open - AI Village

AI Village: Village Open - AI Village
AI vs AI: Securing Telecom in the Era of Autonomous Cyber Warfare - Telecom Village
AI-assisted RF Hacking with GNU Radio - Radio Frequency Village
AImaru C2: La Nueva Era del Living off the Land (MCP AI-Driven C2) - La Villa Community
AIMARU C2: The New Era of LotL (MCP AI-Driven C2) - Red Team Village
AIRGAP BREACHED: Monitoring the Ancestral Payload Leaking from the Poles - Biohacking Village
Alerts and Warnings in 2026 Elections - Voting Village
All About UART - IoT Village
All About UART - IoT Village
All About UART - IoT Village
AMA with EFF - DCNextGen
An Android voyage from Java to Smali with ASM - Mobile Hacking Community
An Intro to Mac Malware Analysis - Malware Village
An Intrusion in the Living Room is now an international incident: SuperBOX Part 3 - Call Center Village
Analyze, Detect & Hunt: Hands-On Malware Analysis, Memory Forensics & AI-Driven Threat Hunting with Endpoint Telemetry - DEF CON Training
Analyze, Detect & Hunt: Hands-On Malware Analysis, Memory Forensics & AI-Driven Threat Hunting with Endpoint Telemetry - DEF CON Training
Anatomy of a Sandworm: A Deep Dive into the Shai-Hulud Attacks - Malware Village
Anomalies Are Not Normal: Election Foam Strikes and the Tragic Story of Mikey Hicks - Voting Village
Anyone Can Hack IoT (Even Easier Now) - A Beginner's Guide to AI Augmented IoT Hacking - IoT Village
AOBTD: AI One Bites The DAST - Demo Labs
AOBTD: AI One Bites The DAST - Demo Labs
Apex Park (Cloud Village CTF) - Contests
Apex Park (Cloud Village CTF) - Contests
Applied SDR Hacking: Red Team SIGINT for mission-critical, automotive, aviation, and marine targets - DEF CON Training
Applied SDR Hacking: Red Team SIGINT for mission-critical, automotive, aviation, and marine targets - DEF CON Training
AppSec Quiz Gauntlet: Spot the Vulnerability - AppSec Village
AppSec Quiz Gauntlet: Spot the Vulnerability - AppSec Village
AppSec Quiz Gauntlet: Spot the Vulnerability - AppSec Village
AppSec Quiz Gauntlet: Spot the Vulnerability - AppSec Village
AppSec Village Tour - The Diana Initiative
Arcade Party - Social Gatherings/Events
Arcanum Security Labs - Noob Community
Arcanum Security Labs - Noob Community
Arcanum Security Labs - Noob Community
Are We Making Things Worse? Election Denialism and Security Research - Voting Village
ARINC 664 CTF Challenge - Aerospace Village
ARINC 664 CTF Challenge - Aerospace Village
ARINC 664 CTF Challenge - Aerospace Village
Assume Breach, But For Real: Rewriting Infrastructure Policy for the Adversaries Who Never Left - Policy @ DEF CON
Atlanta Metro Meetup (DC404/DC678/DC770/DC470) - Social Gatherings/Events
Attack Campaign in VR - Red Team Village
Automated Discovery of Prompt Injection Vulnerabilities via Mutated Prompt Generation - Bug Bounty Village
Automated Mythic Deployment with Gaia - Red Team Village
Autonomous Offense vs. Autonomous Defense: Who's Winning in the Cloud? - Cloud Village
Aviation ISAC Cybersecurity Challenge - Aerospace Village
Aviation ISAC Cybersecurity Challenge - Aerospace Village
Aviation ISAC Cybersecurity Challenge - Aerospace Village
Aw, man...pages! - Contests
AzProwl: Prowling the Azure Attack Surface - Demo Labs
AzProwl: Prowling the Azure Attack Surface - Demo Labs
Badgeliflife Tour - The Diana Initiative
BadVR: Signals Everywhere a collaboration with XR Village - OWASP Foundation
BadVR: Signals Everywhere a collaboration with XR Village - OWASP Foundation

Bait the Bot: Hacking Back Autonomous AI Vulnerability Scanners - La Villa Community
Bashing CloudShells for mining, networking, exfil and persistence at scale - Cloud Village
Battle of the Bots: Vishing Edition - Social Engineering Community Village
BBOT: Automating the OSINT Kill Chain with a Single Command - Recon Village
BBWIC Foundation Tour - The Diana Initiative
Be like a BRAT(BLE Recon and Attack Toolkit): Skip the Handshake, Own the Device - Demo Labs
Be like a BRAT(BLE Recon and Attack Toolkit): Skip the Handshake, Own the Device - Demo Labs
Be your own Agent: Career Journey and Advice from IT and STEM Educator to Cybersecurity Engineer - Noob Community
beacon injected with HOOKCHAIN 2026 - Red Team Village
Beat the Breach: Defend, Respond, Survive - DEF CON Training
Beer Chilling Contraption Contest - Contests
Beer Chilling Contraption Contest - Contests
Beer Chilling Contraption Contest - Contests
Beerus Framework – A New Mobile Framework Arises - Mobile Hacking Community
Behind the Badge: SAOV3 and Open Sourcing the Aerospace Village ISS Badge - Aerospace Village
Beholden to No One: The Nix Override Ladder - Nix Vegas Community
Being Black While Hacking: The Unofficial Survival Guide - Blacks In Cyber Village
Below the Threshold: Real-World APT Tradecraft for Full-Spectrum Compromise - Red Team Village
Better Bug Hunting on AI Products: A VRP Lead's Perspective - Bug Bounty Village
BewAire: Detecting Malicious Pull Requests at Scale with LLMs - Middle Easterns & Africans in Cyber Security (MEACS)
Beyond Heatmaps: Hands-On Cyber Risk Quantification with FAIR - Noob Community
Beyond Normalization: The Expanding Unicode Attack Surface - Bug Bounty Village
Beyond NPPSPY: Harvesting Credentials via Windows Credential Provider Framework - Red Team Village
Beyond Spidering: Behavior Driven DAST for Real Application Workflows - Demo Labs
Beyond Spidering: Behavior Driven DAST for Real Application Workflows - Demo Labs
Beyond the Ceremony: The 2026 Passkey Attack Surface - DEF CON Talks
Beyond the Flag: How CTF Players Become Product Security Engineers - Red Team Village
Beyond the Hype: The Real Role of Red Teams in an AI World - Adversary Village
Beyond Theoretical Risk: How Cache Poisoning Escalated to Critical Account Takeover in TikTok's Web Infrastructure - Bug Bounty Village
Beyond Your Bookshelf: Hackable eReaders - IoT Village
Bias is a Bug: Why Inequality is a Cybersecurity Vulnerability - Blacks In Cyber Village
BIC R00T ACCESS 2026 - Social Gatherings/Events
BIC Village Capture the Flag (CTF) - Contests
BIC Village Capture the Flag (CTF) - Contests
BigIron.ai: AI-Assisted Exploration and Security Analysis of Mainframe Systems - Demo Labs
BigIron.ai: AI-Assisted Exploration and Security Analysis of Mainframe Systems - Demo Labs
Biohacking Device Lab - Biohacking Village
Biohacking Device Lab - Biohacking Village
Biohacking Device Lab - Biohacking Village
Biohacking Village Tour - The Diana Initiative
Bird Hunting Season: The Final Flight - DEF CON Talks
Black Belt Pentesting / Bug Hunting Millionaire: Mastering Web Attacks with Full-Stack Exploitation (100% Hands-On) - DEF CON Training
Black Belt Pentesting / Bug Hunting Millionaire: Mastering Web Attacks with Full-Stack Exploitation (100% Hands-On) - DEF CON Training
Blacks In Cyber Village Tour - The Diana Initiative
BlanketFort Con - Social Gatherings/Events
BLE Theft Auto: How a Dealer-Installed Anti-Theft System Exposes Over a Million Cars to Theft - DEF CON Talks
Blockchain defense, stablecoin attacks, and Web3 OSINT - Cryptocurrency Village
BloodBash: Lightweight CLI Python BloodHound Alternative - Red Team Village
BloodHound OpenGraph Crash Course - Red Team Village
BloodHound OpenGraph: Six Degrees of Everything - Red Team Village
BloodHound Quest - Red Team Village
Blue Team Village CTF - Project Obsidian - Contests

Blue Team Village CTF - Project Obsidian - Contests
Blue Team Village Tour - The Diana Initiative
Blue vs Red Bootcamp: From Attacker Playbooks to Defender Detections - DEF CON Training
Blue vs Red Bootcamp: From Attacker Playbooks to Defender Detections - DEF CON Training
Blue vs Red Bootcamp: From Attacker Playbooks to Defender Detections - DEF CON Training
Blue vs Red Bootcamp: From Attacker Playbooks to Defender Detections - DEF CON Training
BNPL's Blind Spot: Exploiting Business Logic Flaws in Buy Now Pay Later APIs - Payment Village
Bobba! A Complete History of Habbo Hotel Private Servers from Shockwave to HTML5 - Game Hacking Village
Bomb Bot Challenge - Car Hacking Village
Bomb Bot Challenge - Car Hacking Village
Book Signing - Aamiruddin Syed - Social Gatherings/Events
Book Signing - Avinash Majeti - Social Gatherings/Events
Book Signing - Avinash Majeti - Social Gatherings/Events
Book Signing - Avinash Majeti - Social Gatherings/Events
Book Signing - Brandy Smith - Social Gatherings/Events
Book Signing - Brandy Smith - Social Gatherings/Events
Book Signing - Christopher DeCarmen - Social Gatherings/Events
Book Signing - Christopher DeCarmen - Social Gatherings/Events
Book Signing - Cindy Cohn - Social Gatherings/Events
Book Signing - Cindy Cohn - Social Gatherings/Events
Book Signing - Garrett Gee - Social Gatherings/Events
Book Signing - Garrett Gee - Social Gatherings/Events
Book Signing - Laura Scherling - Social Gatherings/Events
Book Signing - Laura Scherling - Social Gatherings/Events
Book Signing - Mark Foudy - Social Gatherings/Events
Book Signing - Nicholas DeMeo - Social Gatherings/Events
Book Signing - Ted Harrington - Social Gatherings/Events
Book Signing - Thomas Wilhelm - Social Gatherings/Events
Bootkits Forever: Emulando APTs Modernos desde UEFI hasta el Kernel - La Villa Community
Bots, Bounties, and Bullshit: An Honest Panel on AI in Hacking - Bug Bounty Village
Break Things, Learn Things: Hands-On Hacking for Beginners (same as Saturday) - Noob Community
Break Things, Learn Things: Hands-On Hacking for Beginners - Noob Community
Breaking and Defending NEURO: Hands-On AI Stack Attack CTF with Cisco Secure AI - Red Team Village
Breaking AWS Bedrock: Novel Attack Techniques Against Cloud Infrastructure - Cloud Village
Breaking BIOS in ATMs - Payment Village
Breaking Ciphers and Zero-Knowledge Proofs - Cryptocurrency Village
Breaking Hardware CFI with Sigreturn - DEF CON Talks
Breaking In, Evil Style: A Guide to Scaring Your CEO - Physical Security Village
Breaking into Amazon lockers by any means necessary - DEF CON Talks
Breaking Local AI Runtimes: Exploiting llama.cpp and Ollama - DEF CON Talks
Breaking MCP Trust Boundaries: Cross-Server Authority Injection in Agent Toolchains - Red Team Village
Breaking PBKDF - Adversarial Cryptanalysis and Techniques for Hunting Cryptographic Flaws - Payment Village
Breaking Physical Access Control: Electrical Fundamentals, RFID Credentials, and Hands-On Offense - DEF CON Training
Breaking Physical Access Control: Electrical Fundamentals, RFID Credentials, and Hands-On Offense - DEF CON Training
Breaking the Chains of Cloud Giants: Building a Fully Autonomous Personal Cloud on NixOS - Nix Vegas Community
Breaking the Cloud Layer - Modern and Practical Attacks on AWS, Azure, GCP, Aliyun, Railway and Vercel - DEF CON Training
Breaking the Cloud Layer - Modern and Practical Attacks on AWS, Azure, GCP, Aliyun, Railway and Vercel - DEF CON Training
Breaking the Ethereum Phone: From BootROM to Wallet Signing Keys - DEF CON Talks
Breaking the Oracle: Building an Offensive Security Toolkit for OCI - Cloud Village
Bricks in the Air - Aerospace Village
Bricks in the Air - Aerospace Village
Bricks in the Air - Aerospace Village
Bridging the GAP: Hands-On Embedded Hardware Hacking - DEF CON Training

Bridging the GAP: Hands-On Embedded Hardware Hacking - DEF CON Training
Bring Your Own Root Of Trust - DEF CON Talks
Bring-Your-Own-EDR - Breaking Windows Process Protection to build EDR-Protected Malware - DEF CON Talks
Bruce's Fireside Chat - AI Village
BTR Reforged: Weaponizing Defender's Remediation Driver as a Kernel Operation Primitive - DEF CON Talks
Bug Bounty Village Closing Ceremony - Bug Bounty Village
Bug Bounty Village CTF - Open - Contests
Bug Bounty Village CTF - Open - Contests
Bug Bounty Village CTF Awards - Contests
Bug Bounty Village Tour - The Diana Initiative
Build Your Own Meshtastic Node: Off-Grid, Encrypted LoRa Meshnets for Beginners! - IoT Village
Build-A-Badge Workshop - Maker's Village
Build-A-Badge Workshop - Maker's Village
Build-A-Badge Workshop - Maker's Village
Building a Hacker Haven: The Long Game of Growing a Local Hacker Community - DEF CON Groups
Building a State Wide VDP: Lessons from Maryland's First Year in the Trenches - Policy @ DEF CON
Building a Strong Community Culture presented by DC407 - DEF CON Groups
Building a Student-Led OSINT Program to Investigate Cryptocurrency Fraud - OSINT For Good Community
Building an open source safecracking robot - Lockpick Village
Building Better Backdoors Than China - Packet Hacking Village
building community and privacy tools from junk - Hackers.town
Building Hackbots - Recon Village
Building Hackbots - Red Team Village
Building Hackbots - AppSec Village
Building Project Obsidian: Designing the Blue Team CTF for DEF CON - Blue Team Village
Building Silkscreens and carving stamps - Maker's Village
Building the Humans Behind the Mission: Talent, Readiness, and Cyber Power for America's Armed Services - Maritime Hacking Village
Building Your First Homelab - Noob Community
Burning Redirectors Before Blue Team Does - Red Team Village
Burp, But Yours: Hands-On Extension and Bambda Development - Bug Bounty Village
Burp, But Yours: Hands-On Extension and Bambda Development - AppSec Village
Bypassing KYC Vendors on AI Times - Mobile Hacking Community
C(2)YA: Inside the Adversary's Inbox - DEF CON Talks
Cache Key Injection: Smuggling Poison Through the Door - Bug Bounty Village
Call Center Tour - The Diana Initiative
Call Center Village - Open - Call Center Village
Call Center Village - Open - Call Center Village
Call Center Village - Open - Call Center Village
Can AI do novel security research? Meet the HTTP Terminator - DEF CON Talks
CAPTURE THE COIN - Announcement of the CTF Winners - Payment Village
Car Hacking Masterclass - Attacking & Defending Automotive Systems and Infrastructure - DEF CON Training
Car Hacking Masterclass - Attacking & Defending Automotive Systems and Infrastructure - DEF CON Training
Car Hacking Village CTF - Contests
Car Hacking Village CTF - Contests
Car Hacking Village CTF - Contests
Car Hacking Village Open - Car Hacking Village
Car Hacking Village Open - Car Hacking Village
Car Hacking Village Open - Car Hacking Village
Car Hacking Village Scavenger Hunt Contest - DEF CON Talks
Car Hacking Village Scavenger Hunt Contest - DEF CON Talks
Car Hacking Village Tour - The Diana Initiative
Cards Against Vulnerabilities - AppSec Village
Cards Against Vulnerabilities - AppSec Village
Cards Against Vulnerabilities - AppSec Village

Cards Against Vulnerabilities - AppSec Village
Cat-apstrophic Hacking: Breaking Into Smart Litter Boxes - IoT Village
Cat-apstrophic Hacking: Breaking Into Smart Litter Boxes - IoT Village
Cat-apstrophic Hacking: Breaking Into Smart Litter Boxes - IoT Village
Catching Cheaters in Super Smash Bros Melee - Game Hacking Village
Catching Cheaters in Super Smash Bros Melee - Game Hacking Village
Certified Re-Pwned: escalating all the way up - DEF CON Talks
Chaining Credentials Through the AI Infrastructure Nobody Secured - Red Team Village
Chaining Logical Bugs for Reliable Windows LPE - DEF CON Talks
Chaining Microsoft Binaries to get Privileged Primitives in the Windows kernel - DEF CON Talks
Chill Zone: Casual Games & TASBot Smash Demo - Game Hacking Village
Chill Zone: Casual Games & TASBot Smash Demo - Game Hacking Village
Chill Zone: Smash (Project Plus) Tournament with Prizes - Game Hacking Village
Chill Zone: Smash (Project Plus) Tournament with Prizes - Game Hacking Village
ChronoRoot: Time-Traveling Through Kernel Trust Boundaries - Blacks In Cyber Village
Cirro: Extending Your Azure Graph Beyond Identities - Cloud Village
Citizen Developers Can't Defend What They Built: Scaling Security Past the Security Team - Cloud Village
Cl0p ^_- Til You Drop - 6 years, 9 Campaigns, 7 0-Days - Recon Village
Clash of Prompts: The World's First Prompt Battle Royale - AppSec Village
Clash of Prompts: The World's First Prompt Battle Royale - AppSec Village
Classic US High Sec: how to pick a Medeco - Lockpick Village
Classical OSINT using AI (Actual Intelligence) - OSINT For Good Community
Cleared for Takeoff: Debunking "Uncertifiable" Cybersecurity - Aerospace Village
Clew: Untangling Evasive Malware with Per-Sample Fuzzing Seeds - Demo Labs
Clew: Untangling Evasive Malware with Per-Sample Fuzzing Seeds - Demo Labs
Click Me: Turning URI Links into Bug Bounty RCE's - Bug Bounty Village
Clone to Pwn: Remote Badge Cloning with the Flipper Zero - Physical Security Village
Closing Talk - Cloud Village
Cloud Forensics 101 : Ghost in the logs - Blue Team Village
Cloud Village CTF: Three Azure Warmups - DCNextGen
Cloud Village Tour - The Diana Initiative
cloud-auth: a provider-agnostic CLI for cross-cloud workload identity - Cloud Village
Cloud-Native C2: Weaponizing Trusted Infrastructure for Initial Access - Red Team Village
CloudBashing: Exploiting free CloudShells for mining, networking, exfil, and persistence at scale - DEF CON Talks
Cloudy with a Chance of Breaches: Hands-On AWS Threat Defense - Cloud Village
Cloudy with a Chance of Venting: Managing Supply Chain Risk - Blue Team Village
CMD+CTRL Cyber Range: DarkMoney - Contests
CMD+CTRL Cyber Range: DarkMoney - Contests
CMD+CTRL Cyber Range: DarkMoney - Contests
Code Cadaver: Break Every System. Save Your Friend. - Contests
Code Cadaver: Break Every System. Save Your Friend. - Contests
Code Cadaver: Break Every System. Save Your Friend. - Contests
Code Invaders: Stop The Insecure Code - AppSec Village
Code Invaders: Stop The Insecure Code - AppSec Village
Code to Cloud: Secure Modern Applications Using Open-Source Tools - AppSec Village
Cold Calls - Social Engineering Community Village
Cold Calls - Social Engineering Community Village
Cold Calls - Social Engineering Community Village
Coloring Reset - Misc
Coloring Reset - Misc
Coloring Reset - Misc
COM Hijacking Voodoo: Tradecraft, Detection Blind Spots, and the COM-Hunter - Red Team Village
Command & Conquer: Hands-on C2 Primer with Mythic - Red Team Village
Commit, Push, Compromise: Attacking Modern GitHub Orgs - Red Team Village
Compiling the World: A Binary Dataset Built from nixpkgs - Nix Vegas Community

Composable Systems with NixOS MicroVMs - Nix Vegas Community
Compounding Interest: Exploiting the ATM Supply Chain - DEF CON Talks
Compounding Interest: Exploiting the ATM Supply Chain - Payment Village
Condense Volumes, Connect Dots, Enrich Contexts: Scaling Root Cause Analysis and Automated Troubleshooting with ML - Middle Easterns & Africans in Cyber Security (MEACS)
Condense, Contextualize, and Correlate: Optimize Costs while Connecting the Dots at Scale - Middle Easterns & Africans in Cyber Security (MEACS)
Conference Planners Meetup - Social Gatherings/Events
Configuring Your Favorite Platforms to Prioritize DNS - Blacks In Cyber Village
Connectivity as Control in the European High North - Policy @ DEF CON
Container Escapes 101 - AppSec Village
Container Escapes Are Not Magic. Here Is How They Actually Work. - AppSec Village
Contest Awards - Contests
Contest Closing Ceremonies & Awards - DEF CON Talks
Control + C = Control Me - Red Team Village
Counting the Dead in the Digital Siege: Detection Infrastructure for Cyber-Mapping Patient Harm - Biohacking Village
Cove: Compositional and Verifiable Confidential Computing Workflows - Crypto & Privacy Village
Covert Quantum Computing - a new quantum security paradigm - Quantum Village
Crack Me If You Can 2026 - Contests
Crack Me If You Can 2026 - Contests
Crack Me If You Can 2026 - Contests
Crack the Core - Contests
Crack the Core - Contests
Crack the Core - Contests
Cracking North Korea's Information Control: How Smugglers, Defectors, and Technologists are Breaking Open the World's Most Locked-Down Information System - DEF CON Talks
Cracking the Cybersecurity Career Code with the Cyber Color Wheel - .EDU Community
Cracking ValleyRAT: From Builder Secrets to Kernel Rootkits - Malware Village
Crafting the Future: DEF CON 34 Light-Up Bow Workshop - Maker's Village
Crash and Compile - Stage Competition - Contests
Crashing the Party: Pwning Control-Flow Integrity with Segmentation Fault-Oriented Programming - DEF CON Talks
Crawlee - Improving crawling with an LLM - Red Team Village
Creator Drop-In - Scambait Village
Creator Talk with RinoaPoison & VanHelen - Scambait Village
CRLF-Powered Desync Attacks: Beheading HTTP streams - DEF CON Talks
Cryptid Hunt - Contests
Cryptid Hunt - Contests
Cryptid Hunt - Contests
Crypto And Privacy Village Tour - The Diana Initiative
Crypto Is Fine. The Code Is Not: Real-World Cryptographic Failures - Crypto & Privacy Village
Cryptocurrency Closing Keynote - Cryptocurrency Village
Cryptocurrency Opening Keynote - Cryptocurrency Village
Cryptocurrency Village Tour - The Diana Initiative
Cryptographer Recruitment: Crack the Substitution Cipher - DCNextGen
Cryptohack Badge Hacking - Cryptocurrency Village
CTF Intro, Quick Guides, and Rule Review - OSINT For Good Community
Ctrl + Alt + Lead: Rebooting Cyber Culture with Human Skills - Noob Community
CTRL the Chaos: When AI Controls Critical Infrastructure - Blacks In Cyber Village
CUDA've done better - Hacking Nvidia GPUs for container-escape and privilege escalation - DEF CON Talks
Cyber & AI Policy Basics: What Every Organization Needs in Place - DEF CON Training
Cyber Deck Competition - Contests
Cyber Deck Competition - Contests
Cyber Deck Competition - Contests
Cyber Gamechangers: Women Who Lead, Secure, and Inspire - Blacks In Cyber Village
Cyber Mirage: Realtime Deepfake Demos - AI Village

Cyber Mirage: Realtime Deepfake Demos - AI Village
Cyber Mirage: Realtime Deepfake Demos - AI Village
Cyber Threat Intelligence 101: From Foundations to AI-Driven Defense - Blue Team Village
Cyberdeck Build - Maker's Village
Cyberdeck Build - Maker's Village
CyberKB: When Your AI Copilot Runs the Recon, Crawls the Dark Web, and Maps the Kill Chain - Recon Village
Damn Vulnerable Agentic AI Application (DVAIA) - Demo Labs
Damn Vulnerable Agentic AI Application (DVAIA) - Demo Labs
Dark Wolf Hack Our Drone Workshop - DEF CON Training
Dark Wolf Hack Our Drone Workshop - DEF CON Training
Darknet Diaries Meet & Greet with Jack Rhysider - DEF CON Groups
Darknet-NG - Contests
Darknet-NG - Contests
Darknet-NG - Contests
DarkSyringe: Automated poisoning of Clinical AI Assistants Through PDFs (a physician's point of view) - Biohacking Village
Data Duplication Village Tour - The Diana Initiative
Data Tomb Raider: Raiding Modern AI Vaults with Legacy Flaws for Treasure Stealing - DEF CON Talks
Day in the Life - Green Beret to AI Penetration Tester - Noob Community
Day of the Dead Hacker Party - Social Gatherings/Events
DC Maker's Community Tour - The Diana Initiative
DC's Next Top Threat Model - Contests
DC's Next Top Threat Model - Contests
DC's Next Top Threat Model - Contests
DC101 - DEF CON Talks
DC702 Meetup - Social Gatherings/Events
DC713 and DC281 - 8th Annual DEF CON Texas Groups Meetup - Social Gatherings/Events
DCG New England Meetup - Social Gatherings/Events
DCNextGen - Bricks in the Air - Aerospace Village
DCNextGen - Bricks in the Air - Aerospace Village
DCNextGen - Bricks in the Air - Aerospace Village
DCNextGen - RIC-1: ELT Localization Exercise - N3VR-G0N Down - Aerospace Village
DCNextGen - RIC-1: ELT Localization Exercise - N3VR-G0N Down - Aerospace Village
DCNextGen - RIC-1: ELT Localization Exercise - N3VR-G0N Down - Aerospace Village
DCNextGen - Space Grand Challenge - SatHack: The MOUSE-1 Mission - Aerospace Village
DCNextGen - Space Grand Challenge - SatHack: The MOUSE-1 Mission - Aerospace Village
DCNextGen - Space Grand Challenge - SatHack: The MOUSE-1 Mission - Aerospace Village
DCNextGen Closing Ceremonies - DCNextGen
DCNextGen Opening Ceremonies - DCNextGen
DCNextGen Party! - Social Gatherings/Events
DDoS Community Tour - The Diana Initiative
DDV open and accepting drives for duplication - Data Duplication Village
DDV open and accepting drives for duplication - Data Duplication Village
DDV open and accepting drives for duplication - Data Duplication Village
De la Explotación de Buffer Overflows al C2 Industrial: Infectando y Controlando RTUs con Malware - La Villa Community
De la nube a la corona: Uso indebido de la identidad híbrida en Azure DevOps Azure, AD, AWS y EKS - La Villa Community
De-Sloppify: Your AI Needs a Proxy - Bug Bounty Village
Dear Red Team, Love Blue Team: Pulling Both Screaming Parties into Purple - The Diana Initiative
Deep Dive into the Dark Web - DEF CON Training
Deep Dive into the Dark Web - DEF CON Training
Deepfake Detection Through Adversarial Research - Payment Village
Deepfake Detection Through Adversarial Research - Payment Village
DEF CON Academy Tour - The Diana Initiative
DEF CON After party @ LIV Fontainebleau - Social Gatherings/Events
DEF CON Beard and Mustache Contest - Contests

DEF CON Closing Ceremonies & Awards - DEF CON Talks
DEF CON CTF: Benevolent Bureau of Birds - Contests
DEF CON CTF: Benevolent Bureau of Birds - Contests
DEF CON CTF: Benevolent Bureau of Birds - Contests
DEF CON Franklin: What worked, what didn't, and how we are giving agency to water utilities at the top of every bad guy's target list because of data centers - DEF CON Talks
DEF CON Groups (DCG) Tour - The Diana Initiative
DEF CON Groups (DCG) - DEF CON Groups
DEF CON Groups (DCG) - DEF CON Groups
DEF CON Groups (DCG) - DEF CON Groups
DEF CON Groups (DCG) - DEF CON Groups
DEF CON Groups Backdoors & Breaches - Contests
DEF CON Groups Backdoors & Breaches - Contests
DEF CON Groups Sticker Contest - Contests
DEF CON Groups Sticker Contest - Contests
DEF CON Scavenger Hunt - Contests
DEF CON Scavenger Hunt - Contests
DEF CON Scavenger Hunt - Contests
Defcon.run - Social Gatherings/Events
Defcon.run - Social Gatherings/Events
Defcon.run - Social Gatherings/Events
Defcon.run - Social Gatherings/Events
Defend zee clankers: OWASP AI Security Verification Standard (AISVS) - OWASP Foundation
Defense in Depth for AI: Launching the AISECA Framework - Middle Easterns & Africans in Cyber Security (MEACS)
Demodus Operandi (Cómo tres rf-hacks en tres bandas terminaron siendo una metodología) - La Villa Community
Demystifying the Playboy RaaS - Malware Village
DeNISTifying Technology: Paradigm Shifting To Quantum Encryption, Post Cryptography, and Digital Forensics - Blacks In Cyber Village
Descubrimiento Industrializado de CVEs con Agentes de IA - La Villa Community
DFMI: Weaponizing MSI Installers for Fileless Code Execution - Red Team Village
DFMI: Weaponizing MSI Installers for Fileless Code Execution - Demo Labs
DFMI: Weaponizing MSI Installers for Fileless Code Execution - Demo Labs
Digital Forensics 101 - Blue Team Village
Digital Modes 101: The Weird, Wonderful World of Computer Radio - Ham Radio Village
Digital Supply Chain Security: Software, Cryptography, AI, and Vendor Risk - DEF CON Training
Direct Network Access for Command and Control - Red Team Village
Disaster Intelligence - The past, present, and future of situational awareness during a crisis - OSINT For Good Community
Disaster Intelligence - The past, present, and future of situational awareness during a crisis - OSINT For Good Community
Discover GE Appliances! - IoT Village
Discover GE Appliances! - IoT Village
Discover GE Appliances! - IoT Village
Dissecting the ICX Frog - Voting Village
Do you feel in control? Analysis of AWS CloudControl API as an attack tool - Red Team Village
Donating Bone Marrow: A Donor's First-Hand Experience - Misc
Dozier Drill Tournament - Contests
DPAPI Is Not a Boundary: A Full Infostealer Kill Chain Operators Can Replicate - Red Team Village
Dr. Strangepwn: How I Learned to Stop Worrying and Love the LLM - IoT Village
Drag, Drop, Deploy, Compromise: Why Trusted HMI Engineering Toolchains Remain an ICS Supply-Chain Blind Spot - Maritime Hacking Village
Dreamcast Ex Inferis — RCE on the Sega Dreamcast PlanetWeb Internet Browser v3.0 - Game Hacking Village
Dreamcast Ex Inferis: RCE on the Sega Dreamcast PlanetWeb Browser - Game Hacking Village
Drive Stats: 14 years of hard drive failure rates - Data Duplication Village
Drive Stats: 14 years of hard drive failure rates - Data Duplication Village
Drogonsec: SAST + SCA + Secrets + IaC in one open-source scanner - AppSec Village
Drone Hacking Choose your Own Adventure - Aerospace Village

Drone Hacking Choose your Own Adventure - Aerospace Village
Drone Hacking Choose your Own Adventure - Aerospace Village
Drone Hacking Workshop - Aerospace Village
Drone Hacking Workshop - Aerospace Village
Drone Hacking Workshop - Aerospace Village
Drone ID on the Wire: RF Detection, Spoofing, and the Limits of Compliance-Based Airspace Awareness - Radio Frequency Village
Drones, Detectors, and the Kill Chain - Aerospace Village
Dylib Hijacking on macOS: Dead or Alive? - DEF CON Talks
Eating Our Own Dogfood: Running a Bug Bounty Program on a Bug Bounty Platform - Bug Bounty Village
EFF Tech Trivia - Contests
El regreso de Sedinho: situación actual y nuevas tácticas de los troyanos bancarios brasileños - La Villa Community
Election Integrity and Technology - Voting Village
Election Observation: Watching is not Enough - Voting Village
Election Security in the Age of AI: Governance, Trust, and the Systems Behind Democracy - Policy @ DEF CON
Embedded - 101 Labs - Embedded Systems Village
Embedded - 101 Labs - Embedded Systems Village
Embedded - 101 Labs - Embedded Systems Village
Embedded & Shredded: Advanced Embedded System Hacking - Biohacking Village
Embedded & Shredded: Advanced Embedded System Hacking - Biohacking Village
Embedded & Shredded: Advanced Embedded System Hacking - Biohacking Village
Embedded System Village Tour - The Diana Initiative
Embedded Systems Village CTF - Embedded Systems Village
Embedded Systems Village CTF - Embedded Systems Village
Embedded Systems Village CTF - Embedded Systems Village
Empire 7: Shipping a C2 at AI Speed - Demo Labs
Empire 7: Shipping a C2 at AI Speed - Demo Labs
Emulating the “Identity-First” Threat Actor: Automated Playbooks for IdP Hijacking - Adversary Village
Escalation Desk CTF - Contests
Escalation Desk CTF - Contests
Escalation Desk CTF - Contests
ESP32 as a counter-surveillance platform - DEF CON Talks
Europe’s Expanding Role in Global Vulnerability Management - Policy @ DEF CON
Evading EDR in ATM - Red Team Village
Evading LLM Detection - Cryptocurrency Village
Every ride you take - Hacking a City’s Public Transportation - AppSec Village
Everything I Need to Know About Security, I Learned from Mr. Rogers - The Diana Initiative
Everything is Nix when you squint hard enough - Nix Vegas Community
Evidence-Based Elections and Risk-Limiting Audits - Voting Village
Evil Is Always a Bad Stylist: .NET Obfuscation with Roslyn - Red Team Village
EvilEssid: Evading Wireless Intrusion Prevention Systems - Red Team Village
Execution of modern techniques to start/improve your career in Incident Response - La Villa Community
Exfil Everything: A Year of Stealing Data from AI Agents - Bug Bounty Village
Exploit Bluetooth Low Energy with BLESPloit and optional ESP32 - Embedded Systems Village
Exploit Bluetooth Low Energy with BLESPloit and optional ESP32 - Embedded Systems Village
Exploit Bluetooth Low Energy with BLESPloit and optional ESP32 - Embedded Systems Village
Exploit Your Own Story - Social Gatherings/Events
Exploit Your Own Story - Social Gatherings/Events
Exploiting Private 5G: Unauthenticated Access to Databases and Control Plane DoS via Fuzzing - Red Team Village
Exploring Security Features in the Armv8-M Architecture - Blacks In Cyber Village
Expose Hidden Surveillance in Everyday Tech - IoT Village
Expose Hidden Surveillance in Everyday Tech - IoT Village
Expose Hidden Surveillance in Everyday Tech - IoT Village
Exposed Data Centers: Bypass IT Security, Crank Up the Heat - ICS Village
Extending Shared Threat Models with the Application Attack Matrix - AppSec Village

Extension Hollowing: Abusing Chrome's Extension Trust Model - Red Team Village
F1NDX OSINT Educational Series - OSINT For Good Community
F1NDX OSINT Educational Series - OSINT For Good Community
F1NDX OSINT Educational Series - OSINT For Good Community
Factory Floor MVP Incident Response Challenge - AppSec Village
Factory Floor MVP Incident Response Challenge - AppSec Village
Falco Hunt: Evading Runtime Detection in Kubernetes - Red Team Village
Farsight: Turning OSINT into Actionable Attack Surface Intelligence - AppSec Village
Feet Feud (Hacker Family Feud) - Contests
Field Notes on Offensive Agents: Reusability, Reliability, and What Breaks - Adversary Village
Filibuffer Overflow: Hackers Stage A Congressional Hearing - Policy @ DEF CON
Finding Bugs Is Easy, Patching Isn't: Build Your Own Remediation Pipeline - AppSec Village
Fireside Chat with Gen. Paul Nakasone - DEF CON Talks
Five Million Industrial Control Systems Walk Into a Bar: What IRONMAP Found When It Scanned the Whole Internet - ICS Village
Fix It, Snooze It, or Ignore It? Cloud Security Decisions Under Pressure - Cloud Village
Flight Simulator/EFB - Aerospace Village
Flight Simulator/EFB - Aerospace Village
Flight Simulator/EFB - Aerospace Village
Flow Like Water: Experiences from Physical Red Teaming - Physical Security Village
Fooling Coding Agents for Fun and Profit - AI Village
For Prompt Injection, Press 1: Hacking AI Voice Agents - Social Engineering Community Village
Forcing Physical Interlocks into Data Transit and Storage Replication - Data Duplication Village
Forcing Physical Interlocks into Data Transit and Storage Replication - Data Duplication Village
Forensics of Covert Entry - Physical Security Village
Forged in fire: Malware Factory - OWASP Foundation
Forget FIPS: An Analysis of Russian and Chinese Cryptographic Standards - Crypto & Privacy Village
Forgotten but Not Gone: Unauthenticated RCEs and LPEs in Legacy Linux Services - DEF CON Talks
FORTRESS Framework - Physical Security Village
Four Newbies Vs. An Insulin Pump. How Hard Can It Be? - Biohacking Village
Fox Hunting - Finding Rogue Access Points in the CTF and in the Wild - Radio Frequency Village
Foxveil: Cloud-Native Loader Tradecraft on Cloudflare, Netlify, and Discord - Cloud Village
Free Ham Radio License Exams - Social Gatherings/Events
Free Ham Radio License Exams - Social Gatherings/Events
Free Ham Radio License Exams - Social Gatherings/Events
Free IP, Free Chaos: DHCP-Assisted Flooding Against Automotive Ethernet - Car Hacking Village
Friends of Bill W - Social Gatherings/Events
Friends of Bill W - Social Gatherings/Events
Friends of Bill W - Social Gatherings/Events
Friends of Bill W - Social Gatherings/Events
Friends of Bill W - Social Gatherings/Events
Friends of Bill W - Social Gatherings/Events
Friends of Bill W - Social Gatherings/Events
Friendship Bracelets - Misc
Friendship Bracelets - Misc
Friendship Bracelets - Misc
From al-Kindi to DEF CON: The Middle Eastern and African Roots of Cybersecurity - Middle Easterns & Africans in Cyber Security (MEACS)
From Application Telemetry Exposure to Cross-Service Pivoting and Full Azure Tenant Takeover - Red Team Village
From Buffer Overflow to Blackout: Chaining Attacks Against Industrial Systems - Red Team Village
From Command Line to Center Stage: Hack Your Way to Confident Speaking - Noob Community
From commit to compromise: securing the full pipeline with AI-assisted remediation - AppSec Village
From Dashboard to Exploit: Weaponizing and Winning the Cloud Queue - Cloud Village
From Disclosure to Defense: Rebuilding Vulnerability Management for the AI Era - Policy @ DEF CON
From Disk Image to ATT&CK in One Binary — a Reference Architecture for Modern Incident Response (in Rust) - Misc

From Findings to Remediations: Open Source Cloud Security at AI Speed with Prowler - Cloud Village
From Fuzzer Noise to a Weaponized PHP Exploit: Exploiting a PHP Use-After-Free Vulnerability - DEF CON Talks
From Kiosk to Domain Compromise: Learning to Walk Up and Take it All - Red Team Village
From Live Malware to Red Team Tradecraft: Process Hollowing in msbuild.exe - La Villa Community
From ONT to STB: Detecting IPTV Attack Chains in the Telecom SOC - Telecom Village
From Path Traversal to Domain Credentials in 90 Seconds - Red Team Village
From Pipeline to Cloud Control - Cloud Village
From Policy to Prod: How a Frontier AI Lab Enforces its Cyber Rules - Policy @ DEF CON
From Practitioner to Principal: Building a Cybersecurity Business That Lasts - Blacks In Cyber Village
From Prompts to Production: Discovering Exposed PII & IDORs in AI-Generated Apps - AppSec Village
From Roots to Renaissance: The Rising Generation of Middle Eastern and African Cybersecurity - Middle Easterns & Africans in Cyber Security (MEACS)
From square root to /root: escalating privileges in Azure containers with Python in Excel - DEF CON Talks
From threat-intel to tested defense, the adversary simulation playbook - Adversary Village
From Wind Farm to CHP Plant: The Untold Story of Lateral Movement in a Polish Energy Sector Attack - DEF CON Talks
From Zero-Day to Zero-Hour: Rethinking Telecom Defense for the Frontier AI Era - Telecom Village
from_pretrained() to from_pwned(): Breaking HuggingFace's Trust - AppSec Village
Front Man's Fête: An Octopus Game Party (including Octopus Game winners and prizes) - Social Gatherings/Events
FTS Build it Yourself: cDc X OWASP X Veilid - OWASP Foundation
Full Disclosure, Full Screen: [Informative] The Story of Bug Bounty Village Badge 2026 - Bug Bounty Village
Full-Stack Pentesting Laboratory: 100% Hands-On + Lifetime LAB Access - DEF CON Training
Full-Stack Pentesting Laboratory: 100% Hands-On + Lifetime LAB Access - DEF CON Training
Fun with alternative smartphones with The Tech Reclaimers! - Hackers.town
Furs and Kinksters Meetup - Queercon Community
Game Hacking Village CTF awards ceremony - Contests
Game Hacking Village CTF Q&A / Walkthroughs - Contests
Game Hacking Village CTF - Contests
Game Hacking Village CTF - Contests
Game Hacking with AI - Game Hacking Village
Game Time: Input, Output, and Variables - CodeBloom
Game Time: Input, Output, and Variables - CodeBloom
Game Time: Input, Output, and Variables - CodeBloom
Game Time: Input, Output, and Variables - CodeBloom
Game Time: Input, Output, and Variables - CodeBloom
Game Time: Loops - CodeBloom
Game Time: Loops - CodeBloom
Game Time: Loops - CodeBloom
Gamer Village Tour - The Diana Initiative
Gamifying the Matrix: a MITRE ATT&CK Video Game - Noob Community
GE(O)SINT Contest - Recon Village
GE(O)SINT Contest - Recon Village
GeoHacking: from memory corruption RCE to cross tenant access - AppSec Village
Geolocating Talent: How OSINT CTFs are Building Tomorrow's Analysts - OSINT For Good Community
Get Set, Exploit! Unveiling Python Class Pollution In-the-Wild - DEF CON Talks
Getting Started in OT/ICS Cybersecurity - Noob Community
Getting Started In Radio Direction Finding - Ham Radio Village
Ghost Followers: Using AI to Unmask Fake LinkedIn Profiles at Scale - Packet Hacking Village
Ghost in the Hiring Machine: How to Spot Fake Personas Before They're on Your Payroll - Recon Village
Ghost in the IDE - Demo Labs
Ghost in the IDE - Demo Labs
Ghost in the Water: Simulating a Nation-State PLC Sabotage Campaign - Red Team Village
Ghost Records: Automating Dangling DNS & Subdomain Takeover Detection at Enterprise Scale - Cloud Village
GhostCatcher (endpoint detection agent) - Demo Labs
GhostCatcher (endpoint detection agent) - Demo Labs
Github Rate Limits Got You Down? FOD's Failing to Build? Let's Talk About Caching - Nix Vegas Community

Give an AI Industrial Protocol Tools and Watch What It Destroys - ICS Village
Global OSINT Search Party CTF – DEF CON 34 Edition - Contests
GnawLab: Open-Source AWS Attack Scenarios Based on Real-World Breaches - Demo Labs
GnawLab: Open-Source AWS Attack Scenarios Based on Real-World Breaches - Demo Labs
Go with the Flow: Riding GCP Dataflow Shadow Dependency to Cross-Tenant Compromise - Cloud Village
Going the Distance: Long-Range Keystroke Injection via Meshtastic - DEF CON Talks
Gold Bug: Puzzle Panel with Friends - Crypto & Privacy Village
Gone in 60 Frames – USB Video Exploitation - DEF CON Talks
Goose Processing Unit (GPU): VRAM as an Unmonitored Attack Surface - Demo Labs
Goose Processing Unit (GPU): VRAM as an Unmonitored Attack Surface - Demo Labs
GOTHCON - Social Gatherings/Events
Gotta Catch 'Em All: How To Capture 3.5 Billion WhatsApp Accounts - DEF CON Talks
Gotta Phish 'Em All! Novel Attack Techniques via Persistent Browser-in-the-Middle - DEF CON Talks
Governing the Firehose: Writing Custom OPA Policies to Tame and Remediate Prowler Output - Cloud Village
gpwn: Wiretapping fiber (GPON) ISP deployments from the comfort of your home - DEF CON Talks
Groking the Kill Chain - Recon Village
Hac-Man - Contests
Hac-Man - Contests
Hac-Man - Contests
Hack the Airwaves – Embedded Wireless for Next-Gen Hackers - DCNextGen
Hack The Box DC Junior Ranger Program Challenge - Noob Community
Hack The Box DC Junior Ranger Program Challenge - Noob Community
Hack The Box DC Junior Ranger Program Challenge - Noob Community
Hack the Duck Store - AppSec Village
Hack the Planet (not ours) - Radio Frequency Village
Hack3r Runw@y v8.0 - Contests
Hackbots - Bug Bounty Village
Hacker Book Club Discussion - Social Gatherings/Events
Hacker Book Club meet up - The Diana Initiative
Hacker Culture 101 - DCNextGen
Hacker Games - Contests
Hacker Games - Contests
Hacker Games - Contests
Hacker Jeopardy - Social Gatherings/Events
Hacker Jeopardy - Social Gatherings/Events
Hacker Karaoke - Social Gatherings/Events
Hacker Karaoke - Social Gatherings/Events
Hacker Runway Crafting Time - The Diana Initiative
Hackers Trivia - Hackers.town
Hackers with Disabilities Tour - The Diana Initiative
HackFortress - Contests
HackFortress - Contests
HackFortress - Contests
Hacking AFDX or Not; A Primer for Flight Control Systems Security - Aerospace Village
Hacking AI - DEF CON Talks
Hacking Airplanes at the NTSB - Aerospace Village
Hacking Android and IOT Apps by Example - DEF CON Training
Hacking Android and IOT Apps by Example - DEF CON Training
Hacking Android Apps in a Structured Way - Mobile Hacking Community
Hacking Cryptography - DEF CON Training
Hacking Cryptography - DEF CON Training
Hacking Education - Teaching Offensive Cyber Science at the Collegiate Level - .EDU Community
Hacking Electronic Conspicuity Devices -or- Making Light Aircraft Fly Into Conflict - Aerospace Village
Hacking GRC Contest - Contests
Hacking GRC Contest - Contests

Hacking GRC Contest - Contests
Hacking Hearts by Reverse Engineering Pacemaker Firmware - Biohacking Village
Hacking Human-in-the-Loop systems - Bug Bounty Village
Hacking IDE Extensions - VSCode Workshop - Bug Bounty Village
Hacking iOS Apps in a Structured Way - Mobile Hacking Community
Hacking Jetskis - from Sea-Don't to Sea-Doo - DEF CON Talks
Hacking the EOD Bot: How I Learned to Stop Worrying and Love the Boomba - DEF CON Talks
Hacking the Government: How Two Researchers Turned Late-Night Boredom Into a National Audit - DEF CON Talks
Hacking the Hackers who Hack Hackers: Supply-Chain Backdoors in Underground VPN Infrastructure - DEF CON Talks
Hacking the Human-in-the-Loop - Red Team Village
Hacking Your Life with AI Can Get You Hacked: How AI Orchestration Platforms Ship RCE by Design - DEF CON Talks
Haetae: An Agent to Takedown North Korean C2 Servers - Adversary Village
Haetae: An Agent to Takedown North Korean C2 Servers - Red Team Village
Haetae: An Agent to Takedown North Korean C2 Servers - Malware Village
Ham In A Day Class - Social Gatherings/Events
Ham Radio - Licensed to Experiment - Ham Radio Village
Ham Radio Isn't Magic: Preppers, Sad Hams, and Practical Off-Grid Communications - Ham Radio Village
Ham Radio Village Tour - The Diana Initiative
Hands-On Autonomous Pentesting with Pentest Copilot - Red Team Village
Hands-On Hardware Hacking – From JTAG to Root, Memory Patching Boot Process for Root Access - IoT Village
Hands-On Hardware Hacking – From JTAG to Root, Memory Patching Boot Process for Root Access - IoT Village
Hands-On Hardware Hacking – From JTAG to Root, Memory Patching Boot Process for Root Access - IoT Village
Hands-On Supply Chain Recon & Vendor Risk Mapping - Recon Village
Hardhat How-to - Maker's Village
Harvest Now, Decrypt Later: Practical Attacks on Post-Quantum Cryptography Implementations - DEF CON Talks
Heavy Metal and Hidden Secrets: A Five-Year Retrospective on DEF CON Challenge Coins - Bug Bounty Village
Hey Adversary, I've Got a Human EDR Bypass for You... - Adversary Village
HHV/SSV Tour - The Diana Initiative
High Voltage Heist: Turning Your EV into my Power Bank - DEF CON Talks
Hook Crook - Extracting More From Discord Webhooks - Demo Labs
Hook Crook - Extracting More From Discord Webhooks - Demo Labs
Hook, Line & Pretext Workshop: Crafting Effective Phish - Social Engineering Community Village
Hostile Input: PDF Triage That Survives an Adversarial Document - Malware Village
How Malicious AI Skills Hijack Your Agents - AppSec Village
How much of our Bluetooth firmware reverse engineering work can now be automated with LLMs? - DEF CON Talks
How Shadow APIs Become an Attacker's Free Pass Into Your Cloud-Native App - AppSec Village
How to destroy a country - Malware Village
How to Epically Fail Your PCI Assessment - Payment Village
How to get RCE on a car - Hackers.town
How to piss off your Nix friends - Nix Vegas Community
How to Profile an entire C-suite in 10 days - OSINT For Good Community
How We Built Xenoptic: A Walkthrough of Design, Infrastructure and Vulns! - Bug Bounty Village
HSPACE: AI Battlegrounds - Contests
HSPACE: AI Battlegrounds - Contests
HSPACE: AI Battlegrounds - Contests
Human in the Loop or Human Out of Luck? - Biohacking Village
Human Registration Open - Social Gatherings/Events
Human Registration Open - Social Gatherings/Events
Human Registration Open - Social Gatherings/Events
Human Registration Open - Social Gatherings/Events
Hunting for Cryptographic Ghosts: A Bug Hunter's Guide to Signature Malleability and Replay Attacks in EVM Bridges & Multi-Sigs - Bug Bounty Village
Hunting the Contagious Trader Delivery Network - Recon Village
I'm Not Special, and You Can Too! A journey into RF Antenna Design for Dummies. - Radio Frequency Village
ICS Village Tour - The Diana Initiative

ICSForge: (Open-Source) OT/ICS Security Coverage Validation Platform - ICS Village
Identity Crisis: Novel Vulnerabilities leading to Kerberos Downgrade, DoS, and Full Domain Takeover - DEF CON Talks
IDEViewer - Securing Developer Workstations from IDE Supply Chain Threats - AppSec Village
If I Were Eighteen Again: Career Advice for the AI Era - Noob Community
Illumicon Tour - The Diana Initiative
Illuminati Party - Social Gatherings/Events
Imposter Syndrome Is Distracting You From the Work That Matters - Noob Community
Improv - Social Engineering Community Village
Improving Security Vulnerability Descriptions using LLMs - Blacks In Cyber Village
In Untrust We Can Trust: Enforcing Trust Boundaries for Humans and AI Alike - AppSec Village
Incident Response 101: Preparing Before the Hack, Responding After It - Blue Team Village
Incident Response in 2026 - Blue Team Village
Industry Challenges & SOC Reality - Telecom Village
Inference in the Infrastructure: Developing NIST AI RMF Resources for Resilient AI in Critical Systems - - Policy @ DEF CON
Influence Operations: Tactics, Defense, and Exploitation - DEF CON Training
Influence Operations: Tactics, Defense, and Exploitation - DEF CON Training
InQuorigible: Quora in Missing Persons OSINT - Recon Village
Inside the Guts of Ransomware - Crypto & Privacy Village
Inside the Red Team Cabal: A Decade of Lessons from Enterprise Red Teams - Red Team Village
Install Me Maybe: Turning Claimable VS Code Extension IDs into Supply-Chain Attacks - DEF CON Talks
Installing and Using the Tracelabs VM - OSINT For Good Community
Intercept.js: Runtime-Aware Detection for JavaScript Environments - Demo Labs
Intercept.js: Runtime-Aware Detection for JavaScript Environments - Demo Labs
Intro to Common Industrial Protocol Exploitation - ICS Village
Intro to Lockpicking - Lockpick Village
Intro to Lockpicking - Lockpick Village
Intro to Lockpicking - Lockpick Village
Intro to Lockpicking - Lockpick Village
Intro to Lockpicking - Lockpick Village
Intro to Lockpicking - Lockpick Village
Intro to Lockpicking - Lockpick Village
Intro to Lockpicking - Lockpick Village
Intro to Scratch - DCNextGen
Introduction to AI-Enhanced Threat Modeling Workshop - AppSec Village
Introduction to Reverse Engineering With Ghidra - Malware Village
Introduction to RFID - Physical Security Village
Introduction to Vulnerable ATM Badge - Payment Village
Introduction to Vulnerable ATM Badge - Payment Village
Introduction to Web Exploitation - Noob Community
iOS Game Hacking : From Zero to GOD Mode - Game Hacking Village
IoT Exploitation Masterclass: Hardware & RF Hacking - DEF CON Training
IoT Exploitation Masterclass: Hardware & RF Hacking - DEF CON Training
IOT Village Tour - The Diana Initiative
Is Your Fridge Running? Then You Better Catch It - State of Security in Refrigeration Systems - ICS Village
IsMyPhonePwned: Analyzing Android/iOS Phones at Scale - Mobile Hacking Community
It's a Payment Terminal. It's My Arcade. It's Everywhere. It Cost Me Nine Bucks. - Payment Village
Jackpotting? Bypass de EDR? - Hacking ATM - La Villa Community
Journey to Create an All-state Cybersecurity Plan for Oklahoma - Policy @ DEF CON
Just Hacking Training - IoT Village
Just Hacking Training - IoT Village
Just Hacking Training - IoT Village
KaliGPT Vibe-Ethical Hacking Session - Blacks In Cyber Village
Kayos Klub - Social Gatherings/Events
Keep the Model on Course: Agentic LLM Workflows for Reversing - La Villa Community

Keeping the Angry Pixies Happy: the Care and Feeding of your Batteries - Ham Radio Village
Key Rotation Won't Save You: Hunting Workload Identity Backdoors in AWS and GCP - Cloud Village
Keychained Melody - Grabbing the Keys to the iCloud Kingdom - DEF CON Talks
Keychecker : SSH Key based attack tool for DVCS Systems - Demo Labs
Keychecker : SSH Key based attack tool for DVCS Systems - Demo Labs
Keynote: Colorado's Creation of RLAs - Voting Village
Killing AI Slop: A Multi-Model Orchestration Framework That Only Reports Findings It Can Prove - Bug Bounty Village
Kryptsec Labs - Noob Community
Kryptsec Labs - Noob Community
Kryptsec Labs - Noob Community
KSCM Scambait Radio - Scambait Village
KSCM Scambait Radio - Scambait Village
KSCM Scambait Radio - Scambait Village
Kubernetes CTF at DEF CON Contest Tour - The Diana Initiative
Kubernetes CTF - Contests
Kubernetes CTF - Contests
Kubernetes CTF - Contests
KYC and XMR... FOR HACKERS! - Hackers.town
L.A.Y.E.R.S - Layered Analysis Engine for Browser Extension Risk and Security - Demo Labs
L.A.Y.E.R.S - Layered Analysis Engine for Browser Extension Risk and Security - Demo Labs
La Rosa de Guadalupe DFIR: Serie de 3 capítulos de misterio Cyber* - La Villa Community
La Villa - Closing Ceremony (ESP) - La Villa Community
La Villa - Opening Ceremony (ESP) - La Villa Community
La Villa Tour - The Diana Initiative
Last chance to pick up drives at the DDV - Data Duplication Village
Latest News in the Proxmark World - Radio Frequency Village
latinas.exe has entered the chat (ESP - POR) - La Villa Community
LaunchBreak: a Sip of Tea, a Click, and a Full Multi-stage Desktop Takeover - DEF CON Talks
Lawyers Meet - Social Gatherings/Events
Learning Deception by Doing: Attacking and Defending - La Villa Community
Legally Hacked: how countries decide when security research Is allowed - Policy @ DEF CON
Leigh Trinity OTW - Malware Village
Lessons from a decade of building whistleblower tech - DEF CON Talks
Lessons Learned From A Decade of Resumes - Noob Community
Lessons Learned from Building a New DEF CON Group presented by DC724 - DEF CON Groups
Lessons Learned from Poland and Beyond: The State of Electric Sector Attacks in 2025 - ICS Village
Let's BLESPl0.it the world together - introducing a new portable Bluetooth Low Energy security tool - Radio Frequency Village
Let's Play! OWASP Cornucopia for Mobile Application Security Threat Modeling - OWASP Foundation
Let's Play! OWASP Cornucopia Threat Modeling - OWASP Foundation
Level Up - Could your Gaming Talents be Perfect for a Career in Cyber Security? - DCNextGen
Leveraging Frida to Bypass Mobile Application Security Controls - Mobile Hacking Community
Leveraging Large Language Models for Policy, Regulatory, and Compliance in IoMT: Opportunities, Risks, and Safeguards - AI Village
LGTM: Bypassing an LLM Build Gate When Prompt Injection Fails - DEF CON Talks
Liberate your Music with Tech Reclaimers - Hackers.town
Liberty and Justice for All - Voting Village
Life Finds a Way: Secure Coding with OWASP ASVS - OWASP Foundation
Lightning Talks and Unconference - Nix Vegas Community
Lightning Talks and Unconference - Nix Vegas Community
Lights Out and Last Call: A Drunken Tabletop on Medical Device Resilience - Biohacking Village
Lights Out: Out-of-Band, Out of Mind, Out of Control - DEF CON Talks
Linecon - Social Gatherings/Events
Live Call Listening - Scambait Village
Live Calls Workshop - Scambait Village

Live Recon Contest — Final Presentations - Recon Village
Live Recon Contest - Recon Village
Live Recon Contest - Recon Village
Living Off Someone Else's Inference - Red Team Village
Living Off Someone Else's Inference - Recon Village
Living Off the IDE: From Initial Access to Covert C2 in Modern AI Code Editors - Red Team Village
Living Off the Vault - Red Team Village
Living Off WebView2: Turning Microsoft's Browser into a Red Team Asset - Red Team Village
LLM-Coached Red Team Tactics to Attack Zero Trust - Red Team Village
Local Language Models in OT - Basics and Considerations - ICS Village
Locked Out? Let's Fix That: An Introduction to the Art of Lockpicking - DCNextGen
Locktopus - Final Championship - Contests
Locktopus - Open Qualifying - Contests
Locktopus - Semi Finals - Contests
Locktopus Challenge Finals - Contests
Logsquashing: Consolidating Relevant Events Logs and Alerts - Middle Easterns & Africans in Cyber Security (MEACS)
LoKi: A LoRa/Meshtastic based implant for Red Teaming - Demo Labs
LoKi: A LoRa/Meshtastic based implant for Red Teaming - Demo Labs
Lonely Hackers Club - CTF Winners Announcement - Lonely Hackers Club
Lonely Hackers Club - Lockpicking Table - Lonely Hackers Club
Lonely Hackers Club - Lockpicking Table - Lonely Hackers Club
Lonely Hackers Club - Lockpicking Table - Lonely Hackers Club
Lonely Hackers Club - Sticker Swap Table - Lonely Hackers Club
Lonely Hackers Club - Sticker Swap Table - Lonely Hackers Club
Lonely Hackers Club - Sticker Swap Table - Lonely Hackers Club
Lonely Hackers Club CTF - Lonely Hackers Club
Lonely Hackers Club CTF - Lonely Hackers Club
Lonely Hackers Club CTF - Lonely Hackers Club
Looking and Peering: Attacking from beyond BGP Adjacency - DEF CON Talks
Low Skill, High Impact Attacks on Internet Voting - Voting Village
Lowering the Orbit: Exploiting Satellite Protocols and communications via Software-Defined-Radio and GS - DEF CON Talks
LSTM Autoencoder Ensemble for NMEA 2000 Intrusion Detection on Vessel Networks - Maritime Hacking Village
Lyra: An LLVM IR Obfuscator for Rust - Malware Village
M0us3: A Lightweight, Multi Session C2 Framework with a Rust based Windows Implant - Red Team Village
macOS Doesn't Get Malware...Until It Does - Red Team Village
MailX-Ray: A TSA X-Ray for Emails — Air-Gapped Safe-Read and Quick Triage in an Ephemeral MicroVM - Demo Labs
MailX-Ray: A TSA X-Ray for Emails — Air-Gapped Safe-Read and Quick Triage in an Ephemeral MicroVM - Demo Labs
Make Money Hacking AI - Bug Bounty Village
Make your very own evil IoT Cat Lamp with WLED! - IoT Village
Make your very own evil IoT Cat Lamp with WLED! - IoT Village
Makers' Village - Hacker Arts and Crafts - Maker's Village
Makers' Village - Hacker Arts and Crafts - Maker's Village
Makers' Village - Hacker Arts and Crafts - Maker's Village
MalSkill Lab: Hands-On Natural Language Malware in AI Agent Orchestration Systems - Demo Labs
MalSkill Lab: Hands-On Natural Language Malware in AI Agent Orchestration Systems - Demo Labs
MalSkill: Weaponizing AI Agent Skills for Persistence, Exfiltration, and Lateral Movement - Red Team Village
Malware Inc.: Cybercrime-as-a-Service y la economía del cibercrimen moderno - La Villa Community
Malware Village Tour - The Diana Initiative
Malysis: A Bare-Metal RAM Enclave for Malware Analysis. No Hypervisor. No Trace. - Social Gatherings/Events
Malysis: A Bare-Metal RAM Enclave for Malware Analysis. No Hypervisor. No Trace. - Social Gatherings/Events
Man-in-the-Browser: Hijacking Javascript APIs for Browser Persistence and Credential Theft - AppSec Village
Maritime Hacking Village Policy Panel: Shadow Fleets, Cyber Effects, and Plausible Deniability - Maritime Hacking Village
Maritime Hacking Village Policy Panel: Subsea Cables as Strategic Chokepoints - Security, Sovereignty, and the Grey Zone - Maritime Hacking Village

Maritime Hacking Village Tour - The Diana Initiative
Maritime Threat Hunting: What We Actually Find When We Look - Maritime Hacking Village
MCP Servers: The Next Enterprise Attack Surface - Red Team Village
MCPwned: How Exposed AI Agents Became the Internet's New Recon Toy - Adversary Village
MEACS Trivia, Games and Networking - Middle Easterns & Africans in Cyber Security (MEACS)
MEACS Trivia, Games and Networking - Middle Easterns & Africans in Cyber Security (MEACS)
MEACS: Middle Easterns & African in Cyber Security Tour - The Diana Initiative
Meet XEntry Team: A powerful threat actor abusing Bitlocker for ransomware - La Villa Community
Memory Laundering via Metal: What EDR Can't See on Your Mac - DEF CON Talks
Men Loving Men Meetup - Queercon Community
Mentoring and Career Advice - Noob Community
Mentoring and Career Advice - Noob Community
Mentoring and Career Advice - Noob Community
Merch (formerly swag) Area Open -- README - Social Gatherings/Events
Merch (formerly swag) Area Open -- README - Social Gatherings/Events
Merch (formerly swag) Area Open -- README - Social Gatherings/Events
Mesh Nets for Hackers: How (& When) to use Meshtastic, Meshcore, & Reticulum! - IoT Village
Mesh Nets for Hackers: How (& When) to use Meshtastic, Meshcore, & Reticulum! - IoT Village
MeshLens: Security Profiling at Scale - AI Village
Meshpocalypse: Building Your Own Off-Grid Hacker Network - DCNextGen
Meshtastic 101: Off-Grid Mesh Networking with LoRa - Ham Radio Village
Meshtastic Beasts and Where to Find Them - Ham Radio Village
Microsoft and Amazon are my Favorite C2 Providers - Adversary Village
Microsoft and Amazon are my Favorite C2 Providers - Red Team Village
Minimal by Design: Building Hardened Near-Zero-CVE Container Images - Cloud Village
Minimize Harm, Maximize Defense: How Anthropic Navigates the Offense-Defense Divide - AI Village
Mission: Compromised - Hacking a Satellite from the Ground Up - Aerospace Village
Mission: Compromised - Hacking a Satellite from the Ground Up - Aerospace Village
Mission: Compromised - Hacking a Satellite from the Ground Up - Aerospace Village
Mobile Hacking - Informal CTF - Mobile Hacking Community
Mobile Hacking - Informal CTF - Mobile Hacking Community
Mobile Hacking - Informal CTF - Mobile Hacking Community
Mobile Hacking Community - Open - Mobile Hacking Community
Mobile Hacking Community - Open - Mobile Hacking Community
Mobile Hacking Community - Open - Mobile Hacking Community
Mobile Hacking Tour - The Diana Initiative
Mobile Security through Obscurity, from insecure client-side encryption to unauthenticated SQL - Mobile Hacking Community
Monitor, Compile, Enforce: A Compiler Pipeline for Container Security Policy in Rust and eBPF - Demo Labs
Monitor, Compile, Enforce: A Compiler Pipeline for Container Security Policy in Rust and eBPF - Demo Labs
Monocultures Are Vulnerabilities: Representation and Security in STEM - Blacks In Cyber Village
Morbidity and Mortality: Hackers, HIPAA, and a new Prescription for Healthcare Cyber Policy - Policy @ DEF CON
Most threat modeling artifacts don't help coding agents fix business logic. Here's what does. - AppSec Village
MOUSE Runner & Flappy Drone - Aerospace Village
MOUSE Runner & Flappy Drone - Aerospace Village
MOUSE Runner & Flappy Drone - Aerospace Village
Movie Night - Social Gatherings/Events
Movie Night - Social Gatherings/Events
MSCodePhish: Redeem Your Coupon. Surrender Your Session - Demo Labs
MSCodePhish: Redeem Your Coupon. Surrender Your Session - Demo Labs
MSIX'd Up: Weaponizing the Modern Windows App Packaging Ecosystem - DEF CON Talks
Music - Genre: Breakbeats - Social Gatherings/Events
Music - Genre: Breakbeats - Social Gatherings/Events
Music - Genre: Drum & Bass - Social Gatherings/Events
Music - Genre: Drum & Bass - Social Gatherings/Events

Music - Genre: Drum & Bass - Social Gatherings/Events
Music - Genre: Drum & Bass - Social Gatherings/Events
Music - Genre: Dubstep - Social Gatherings/Events
Music - Genre: Electro House - Social Gatherings/Events
Music - Genre: Goth / Industrial - Social Gatherings/Events
Music - Genre: Goth / Industrial - Social Gatherings/Events
Music - Genre: House - Social Gatherings/Events
Music - Genre: House - Social Gatherings/Events
Music - Genre: Nerdcore - Social Gatherings/Events
Music - Genre: Nerdcore - Social Gatherings/Events
Music - Genre: Techno - Social Gatherings/Events
Music - Genre: Techno - Social Gatherings/Events
Music - Genre: Techno - Social Gatherings/Events
Music - Genre: Trance - Social Gatherings/Events
Music - SomaFM - Social Gatherings/Events
Music - SomaFM - Social Gatherings/Events
Music - SomaFM - Social Gatherings/Events
Music - SomaFM - Social Gatherings/Events
Nation State Obfuscation Networks - Telecom Village
Navigating AI-Assisted Submissions - Bug Bounty Village
Nebula - 5 years, still kicking *aaS - Cloud Village
Nebula Showdown: Space Systems Security CTF Adventure - Aerospace Village
Nebula Showdown: Space Systems Security CTF Adventure - Aerospace Village
Nebula Showdown: Space Systems Security CTF Adventure - Aerospace Village
Neotropolis: The Making of the Railgun Trackers - Radio Frequency Village
Network Implants: Lessons Learned Building Reliable Red Team Dropboxes - Red Team Village
New AWS IAM Attack Paths and the Framework to Exploit Them - Cloud Village
Nix Knows When the Agent Is Wrong - Nix Vegas Community
Nix Vegas Closing Ceremony - Nix Vegas Community
Nix Vegas Opening Ceremony - Nix Vegas Community
Nix Vegas Opening Ceremony - Nix Vegas Community
NixOS Workspaces - Nix Vegas Community
No Entry: Badge Access Denial on Demand - Physical Security Village
No Jailbreak Required: Pwning AI Agents Through the Tools They Trust - AppSec Village
No One Makes It Alone - Community as the Ultimate Security Control - Noob Community
No Prompt Required: Pre-Task RCE in Google Gemini CLI - DEF CON Talks
No Socket, No Privs, No Problem: Weaponizing OCI Registries for SSRF, Credential Theft, and Container Escapes - DEF CON Talks
No Stupid Questions - Noob Community
No Stupid Questions - Noob Community
No Stupid Questions - Noob Community
Non-Binary/Gender Non-conforming Meetup - Queercon Community
Noob Community - Conference Closing - Noob Community
Noob Community - DEF CON 34 Opening Statements - Noob Community
noRecognition: Could a pattern on your clothing fool Facial Facial Recognition? - DEF CON Talks
North Korea's Zoo: Poaching for Gophers, Armadillos and RATs - Malware Village
Not Your Parents' Schoolhouse Rock: Getting Tech Policy Done in a Non-Functioning Congress - Policy @ DEF CON
Nothing Wrong Here: Why AI Artifact Scanners Wave Malware Through - Middle Easterns & Africans in Cyber Security (MEACS)
Novice design in 3d space - Maker's Village
NPM Imposters - The malware detection card game - AppSec Village
NPM Imposters - The malware detection card game - AppSec Village
Nuclear Industrial Control System Simulation (NICSSIM) aka Multi-Agent Cyber Defense Framework for Distributed
Nuclear Operational Technology Systems - ICS Village
O Lado Sombrio das Coisas: Transformando Dispositivos DIY em Vetores de Ataque - La Villa Community

OASIS: Prompt to Pwn - Noob Community
Objectively Awesome Robots: A Hands-On Introduction to Python Classes and Objects - DCNextGen
OCIguana - A vulnerable-by-design OCI lab - Cloud Village
Octopus Game - Booth Battle #1: The Front Man's Wager - Contests
Octopus Game - Booth Battle #2: The Midnight "Brawl" - Contests
Octopus Game - Booth Battle #3: The Marbles Match - Contests
Octopus Game - Booth Open - Contests
Octopus Game - Booth Open - Contests
Octopus Game - Opening Ceremony - Contests
Octopus Game - The Final Booth Battle - Contests
Octopus Game - Walk-In Registration (Pre-Registration Check-In Closed) - Contests
Octopus Game - Walk-In Registration (Pre-Registration Check-In Closed) - Contests
Octopus Game Opens and Pre-registration Check-In Available - Contests
Offensive Cyber Security Operations: Mastering Breach and Adversarial Attack Simulation Engagements - DEF CON Training
Offensive Cyber Security Operations: Mastering Breach and Adversarial Attack Simulation Engagements - DEF CON Training
Offensive Security from Your Pocket - Mobile Hacking Community
OffGuard: Breaking the Most Popular AI Gateway from Auth Bypass to Cloud Compromise - DEF CON Talks
Oh hai! Meet Jason Haddix - OWASP Foundation
Oh hai! Meet Tanya "SheHacksPurple" Janca - OWASP Foundation
On the Weaponization of Voting Channels - Voting Village
Once Upon a Prompt: Fairy Tales That Explain AI Security - Middle Easterns & Africans in Cyber Security (MEACS)
One Chain to Own Them All — Breaking AI Infrastructures - DEF CON Talks
One Firmware Flaw, 70+ Device Models: Lessons in Industrial IoT Disclosure and Mitigation - IoT Village
One Request to Rule Them All - Red Team Village
Open Q&A - Scambait Village
Open Q&A - Scambait Village
Open Q&A - Scambait Village
Opening Panel - "Is Red Teaming Dead?" - Red Team Village
Opening Talk - Cloud Village
Operation Restoration - Maker's Village
Operator, Please Hold - DCG Social - Social Gatherings/Events
OSINT for Hackers Redux - Red Team Village
OSINT Is Still a Thinking Game: Surviving AI Without Losing Tradecraft - Recon Village
OSINT Search party CTF Debrief - OSINT For Good Community
OSINT Search Party CTF Prize and Award Announcements. - OSINT For Good Community
OSINT: Zero To Hero - Noob Community
OSINT4Good Community - DC NextGen Content - OSINT For Good Community
OSINT4Good Community - DC NextGen Content - OSINT For Good Community
OSINT4Good Community - DC NextGen Content - OSINT For Good Community
OSINT4Good Sticker Swap - OSINT For Good Community
OSINT4Good: What it takes to find missing people - OSINT For Good Community
OT Round table. Real talk on how to protect your OT spaces - ICS Village
OT Segmentation Under Operational Constraints - ICS Village
Ouroboros Attack! Recursive AI-Assisted 0-Day Hunting - Red Team Village
Overcast: Video OSINT Agent. Point It at 100 Videos, Ask Anything - Demo Labs
Overcast: Video OSINT Agent. Point It at 100 Videos, Ask Anything - Demo Labs
OWASP AIBOM Generator - AppSec Village
OWASP Amass v5.0 - OWASP Foundation
OWASP Chapter Meetup - OWASP Foundation
OWASP CTF: Getting started & welcome - Contests
OWASP CTF - Contests
OWASP CTF - Contests
OWASP FinBot CTF: Hands-On Agentic AI Threats - AppSec Village

OWASP ISTG in Practice: A CTF-Style IoT Hacking & Defending Lab - OWASP Foundation

Own the con - Queercon Community

Packet Hacking Village Tour - The Diana Initiative

Party Line (Call Center Village Party) - Social Gatherings/Events

Past the Bouncer: The Limits of CSP, Eleven Years In - AppSec Village

Patch Gap to Mobile Renderer RCE: Pwning Samsung Internet's V8 on the Galaxy S25 - DEF CON Talks

Patch Me If You Can: Hands-On Network Threat Defense - Cloud Village

Pattern, Graph, Prompt: What Happens When You Layer Three Analysis Paradigms on the Same Codebase - AppSec Village

Payment Village Intro - What's Happening at the Village - Payment Village

Payment Village Intro - What's Happening at the Village - Payment Village

Payment Village Tour - The Diana Initiative

Peekaboo: Breaking the Black Box of Threat and Malware Emulation - Demo Labs

Peekaboo: Breaking the Black Box of Threat and Malware Emulation - Demo Labs

Pentester vs AI: Race The Machine, In Real Life - AppSec Village

PentestGPT: The Art of Hacking with Words - La Villa Community

Pentesting made easy - Keeping sessions alive with session chains - AppSec Village

Phasmid: Deniable Storage for Rubber-Hose Scenarios - Demo Labs

Phasmid: Deniable Storage for Rubber-Hose Scenarios - Demo Labs

PhreakMe - Contests

PhreakMe - Contests

PhreakMe - Contests

Physical Security is not sexy which is bad for organizations and good for red teams. - Physical Security Village

Physical Securty Village Tour - The Diana Initiative

Pickled and Exposed: RCE in AI Serving Frameworks - AppSec Village

Pickpocketing for Red Teamers: A Hands-On Experience - Social Engineering Community Village

Pinball High Score Contest - Contests

Pinball High Score Contest - Contests

Pinball High Score Contest - Contests

Pinchy Gets Played: How We Red-Teamed AI Agents Before the Threats Did - Cloud Village

Playing with Hyper-local Pocket-Sized Servers - IoT Village

Please Place Your Electronic Devices in {Maritime} Mode: Exposing NTN's Maritime Attack Surface - Maritime Hacking Village

Plug And Pwn: Weaponizing Windows PnP Auto-Install - DEF CON Talks

PMTC: One-Click RCE and Persistent Exfil in AI Coding Agents - Red Team Village

Point of Failure: Autopsia de una Terminal de Pago - La Villa Community

Poison the Well: RAG Attacks Against the Hacking Community's Own Archives - Data Duplication Village

Policy @ Defcon Tour - The Diana Initiative

Policy Mixer Happy Hour - Social Gatherings/Events

Polycon - Queercon Community

Poor Man's Mythos: Signal Siege: Agentic Exploit Chains Across the 5G Cloud-Native Stack - Telecom Village

Post-Exploitation of the Desktop with JS-Tap - Red Team Village

Poster Presentations - AI Village

Poster Presentations - AI Village

Practical AI Security Assessments Using OWASP AISVS - OWASP Foundation

Practical Cybersecurity Skills in an AI-Augmented World: Protecting the AI Trifecta - Noob Community

Practical Guidance for RF Researchers: Experiment First, Interfere Never - Radio Frequency Village

Practical Privacy Defenses for the Paranoid - OSINT For Good Community

Praetor: An OPSEC Exposure Advisor for Empire Operators - Red Team Village

Precogly: Open-Source Threat Modeling for the AI-Coding Era - AppSec Village

Privacy You Inherit: How Cultural History Writes the Source Code for AI Surveillance Policy - Policy @ DEF CON

Privacy's Defender with Women in Security and Privacy (WISP) - Misc

Privacy's Defender: How Hackers Protected the Internet Before and Can Do It Again - Policy @ DEF CON

Privilege Escalation: A Career Story - Noob Community

Privilege Escalation: Building a Cyber Career with Zero Support - Noob Community

Proactive Malicious Package Defense - AppSec Village

Prompt Injection Detection in Large Language Models: Survey and Evaluation of Open Source Tools - Blacks In Cyber Village

Prompt Injection: Attacking and Defending AI-Powered Applications - AppSec Village

PromptPwn: Finding and Exploiting AI-Generated Vulnerabilities at Scale - Demo Labs

PromptPwn: Finding and Exploiting AI-Generated Vulnerabilities at Scale - Demo Labs

Protecting Humans at Machine Speed - Engineering AI to Stop Spam, Scams & Digital Fraud at Telecom Scale - Telecom Village

Pub Quiz at DEF CON - Contests

Publicly Auditable Elections - Voting Village

Pulling Back the Curtain on the Voting Booth - Voting Village

PurpleLoop: Closing the Loop Between Detection Rules, Log Schemas, and Purple-Team Validation - Cloud Village

PWN UR H0M3 - DDoS CTF - Contests

PWN UR H0M3 - DDoS CTF - Contests

PWN UR H0M3 - DDoS CTF - Contests

PWN UR H0M3 DDoS CTF Winner Announcements - Contests

Pwning Agentic Browsers with PleaseFix: A New Vulnerability Class for 0-Click Takeover - AI Village

Pwning Rekordbox: Unauthenticated filesystem access in the world's most popular DJ software - DEF CON Talks

Pwning the Internet of Agents: Zero-Click Backdoors in OpenClaw and a Global Agent Botnet on MoltBook - AI Village

pymisi: Interactive MSI Installer Analysis in Python and the Browser - Demo Labs

pymisi: Interactive MSI Installer Analysis in Python and the Browser - Demo Labs

Pyramid of Pain-Red Team (Human and Technical Friction) - Red Team Village

Q-Day - the Early Years... - Quantum Village

Q&A with the "How to Profile an entire C-suite in 10 days" speaker - OSINT For Good Community

Q&A with the Classical OSINT Using AI speaker - OSINT For Good Community

Q&A with the OSINT4Good Panel - OSINT For Good Community

Quality over Quantity: How to Publish CVEs that Actually Matter - Red Team Village

Quantum Computing The Game Changer You Can t Ignore - Blacks In Cyber Village

Quantum Village Tour - The Diana Initiative

Quantum-Ready or Not: What 1,000 Codebases Reveal About Cryptographic Risk - Crypto & Privacy Village

Queercon Community Lounge Tour - The Diana Initiative

Queercon Mixer - Social Gatherings/Events

Queercon Mixer - Social Gatherings/Events

QueerCon Opening Meet and Greet - Queercon Community

Quiet Room - The Diana Initiative

Quiet Room - The Diana Initiative

Quiet Room - The Diana Initiative

Quiet Room - The Diana Initiative

Racing PX4: Memory Safety and Timing Vulnerabilities - Aerospace Village

Radio Frequency Capture the Flag - Contests

Radio Frequency Capture the Flag - Contests

Radio Frequency Capture the Flag - Contests

Radio Frequency Capture the Flag - Contests

Radio Frequency Village Events - Radio Frequency Village

Radio Frequency Village Events - Radio Frequency Village

Radio Frequency Village Events - Radio Frequency Village

Radio Frequency Village Tour - The Diana Initiative

Rage Against the Sandbox: Bypassing Apple's iOS Security to Run Unsigned Code via SSH - DEF CON Talks

Raiders of the Lost Firmware: A Hands-On Workshop in IoT Firmware Archaeology - IoT Village

Raiders of the Lost Firmware: A Hands-On Workshop in IoT Firmware Archaeology - IoT Village

Raiders of the Lost Firmware: A Hands-On Workshop in IoT Firmware Archaeology - IoT Village

Raiders of the Lost Firmware: A Hands-On Workshop in IoT Firmware Archaeology - IoT Village

Raitlin's Challenge - Contests

RASM: A State Machine Methodology for RF Security Assessment - Radio Frequency Village

Real7y Overrun - Contest running - Contests

Real7y Overrun - Contest running - Contests

Real7y Overrun - Contest running - Contests
Rebuilding Code Security with Signal, Speed and AI - AppSec Village
Recon on Trial: The OSINT Operator's Legal Playbook - Recon Village
Recon Village Tour - The Diana Initiative
Red Robin: Don't Hack For Me, Hack With Me - La Villa Community
Red Team Express - Red Team Village
Red Team Village Tour - The Diana Initiative
Red Teaming Kubernetes: From App-Level CVEs to Full Cluster Takeover - Red Team Village
RedMatter: Let AI Write Your Cross-Platform Mobile Exploits - Mobile Hacking Community
redStack: Boot-To-Breach Red Team Platform - Red Team Village
redStack: Boot-to-Breach Red Team Platform - Noob Community
Reflections on Disregarding Trust (Weaponizing CDP and MHTML for Header-Agnostic Session Hijacking) - DEF CON Talks
Relocatable Nix Binaries - Nix Vegas Community
Requiem for the Decommissioned: When Dead Hosts Bite Back - Red Team Village
Resume Review with the Lonely Hackers Club - Lonely Hackers Club
Resume Review with the Lonely Hackers Club - Lonely Hackers Club
Return of Sedinho: Current situation and new tactics of the Brazilian banking trojan ecosystem - Malware Village
Return of the Defender: Using AI to Strike Back Against Enterprise Threats - Blacks In Cyber Village
Reversing a Recall: From 'Noise Triggered' to RCE - DEF CON Talks
Reversing F5: Pure-Go Steganography, Live Forensic Cover Recovery, and JPEG Fragility Analysis - Demo Labs
Reversing F5: Pure-Go Steganography, Live Forensic Cover Recovery, and JPEG Fragility Analysis - Demo Labs
RF CTF and World Wide War Drive Outbrief - Radio Frequency Village
RF CTF Kick Off Day 1 - Radio Frequency Village
RF CTF Kick Off Day 2 - Radio Frequency Village
RFID Bootcamp: Unleashed! - Red Team Village
Riding for Free - Breaking Public Transport RFID at Scale - DEF CON Talks
Riot Games Vanguard: Pwn to own - Game Hacking Village
Riot Games Vanguard: Pwn to own - Game Hacking Village
RIP Denuvo: DRM in a Post-Hypervisor World - Game Hacking Village
Robot Hacking Community Tour - The Diana Initiative
Root Access: An APT Analysis of Systemic Gatekeeping in Cybersecurity - Blacks In Cyber Village
Root From Kilometers Away: Ubiquiti AirMax RCE - DEF CON Talks
Root-as-a-Service: The Hidden Runtime of Azure AI Foundry - Cloud Village
ROP for the Web: Smuggling XSS, SQLi, and Web Shells Past Every WAF Using Compression Dictionaries - AppSec Village
Ropkit: Framework for Windows Kernel Code Execution under HVCI - Malware Village
Running a homelab with NixOS - Nix Vegas Community
Running your own LTE network for fun and profit???? - Radio Frequency Village
SADF: A Taxonomy and Evaluation Framework for Agentic Security Failures - AI Village
Safe, Secure, and Effective: What Static Behavior Analysis Reveals About the Software Running Your Medical Devices - Biohacking Village
SANS Institute NetWars Labs - Noob Community
SANS Institute NetWars Labs - Noob Community
SANS Institute NetWars Labs - Noob Community
Satellites Under Attack: Hands-On Satellite Security Threat Scenarios - Aerospace Village
Satellites Under Attack: Hands-On Satellite Security Threat Scenarios - Aerospace Village
Satellites Under Attack: Hands-On Satellite Security Threat Scenarios - Aerospace Village
SBOM Find the Flaws - AppSec Village
SBOM Find the Flaws - AppSec Village
SBOM Find the Flaws - AppSec Village
SBOM Find the Flaws - AppSec Village
Scaling Adversary Emulation with Autonomous Agents - AI Village
Scambait Bingo - Scambait Village
Scambait Community Tour - The Diana Initiative

ScamBusters: Turning Undergrads into Threat Hunters - .EDU Community
Scammers Don't Discriminate - Scambait Village
Scuttling Dashboards - Maritime Hacking Village
SE Improv - Social Engineering Community Village
search_vulns: Navigating the Fragmented Landscape of Vulnerability Data - AppSec Village
SEC Vishing Competition (SECVC) - Contests
SEC Vishing Competition (SECVC) - Contests
SecKC the WHOLE WIDE WORLD - Social Gatherings/Events
SecretSifter: Production Apps Are Leaking Credentials. The Blindspot DAST Never Checked. - Demo Labs
SecretSifter: Production Apps Are Leaking Credentials. The Blindspot DAST Never Checked. - Demo Labs
Securing Nix Builds using microVMs - Nix Vegas Community
Securing the AI Stack and Hunting Across Clouds - Cloud Village
Securing the Future: Defending Kubernetes & Cloud-Native Infrastructure in the Age of AI - DEF CON Training
Securing the Future: Defending Kubernetes & Cloud-Native Infrastructure in the Age of AI - DEF CON Training
Securing the Safety Net: Why Healthcare Cybersecurity Policy Keeps Failing Patients - Policy @ DEF CON
Security Analysis of Open-Source Software Used in Onboard Satellite Systems - Aerospace Village
Security and Privacy for the Rest of Elections - Voting Village
Security at Machine Speed: How Autonomous AI Agents Are Changing Cloud Defense - Cloud Village
Security Vulnerabilities in SATCOM Devices - Radio Frequency Village
Self Hosting Nightmare - Exploiting AI models for supply chain attacks - La Villa Community
SEND: Teaching Machines to Lie to Defenders - Adversary Village
Senrigan () x Suzaku (): Threat Hunting & DFIR for AWS — No SIEM, Just Your Laptop - Demo Labs
Senrigan () x Suzaku (): Threat Hunting & DFIR for AWS — No SIEM, Just Your Laptop - Demo Labs
Separating News from Noise - Voting Village
SH4ZAM: Accelerated Vector Math on the Sega Dreamcast - Game Hacking Village
Shadow Webhooks: Hunting for Dangling Event Listeners in Enterprise Workspaces - Bug Bounty Village
Shapeshifting C2: Applying DAITA Traffic Shaping to Defeat DPI and DLP Detection - Red Team Village
Shepherding the Tor network - DEF CON Talks
Shipcrawler: Automated Maritime OSINT — From Open Data to Actionable Intelligence - Maritime Hacking Village
Shopping Is The Attack: A Decade Of E-Commerce Scalper Wars, And The Multi-Agent AI Era - DEF CON Talks
Sick Signals: Adversarial Prompt Injection via Medical IoT Telemetry - IoT Village
Signal Hijacked: How Mobile Networks Became Phishing's Most Trusted Delivery Layer - Telecom Village
Signaling Sabotage: Why 100% Compliance is 0% Security - Telecom Village
SIM Card Strikes Back: Telecom Threats & SOC Detection - Telecom Village
Simulated Adversary: Tactics & Tools Training - DEF CON Training
Simulated Adversary: Tactics & Tools Training - DEF CON Training
sisakulint:CI-Friendly static linter with autofix, SAST, semantic analysis for GitHub Actions - Demo Labs
sisakulint:CI-Friendly static linter with autofix, SAST, semantic analysis for GitHub Actions - Demo Labs
Six Impossible Things Before Breakfast: Common Misconceptions About Being a CTI Analyst - Noob Community
Skill Issue: A Recon Story - Bug Bounty Village
Skillbit Labs - Noob Community
Skillbit Labs - Noob Community
Skillbit Labs - Noob Community
Skimmers, Shimmers, and You - Payment Village
Sliding into the Flight Deck's DMs: Practical Message Attacks on CPDLC - DEF CON Talks
Slop Spotting, Using Rules to Detect AI Slop for Bug Bounty - Bug Bounty Village
Slopcon - Social Gatherings/Events
Smart Contracts, Smarter Malware: Automating Recon on Blockchain-Based C2 - Malware Village
Smart Home in the Matter: Blink, Race, Attack CTF - IoT Village
Smart Home in the Matter: Blink, Race, Attack CTF - IoT Village
Smart Home in the Matter: Blink, Race, Attack CTF - IoT Village
Smile, you're on camera! Livestreaming from North Korea's IT workers laptop farm - DEF CON Talks
Snap, Crackle, Popped: How to manage a massive cyber attack - Biohacking Village
So You Got Your License, Now What? - Ham Radio Village
So You Want to Be a Red Teamer? The Reality Behind the Role - Noob Community

So You Want to Work in Aircraft Cyber? Here's what you need to know! - Aerospace Village
SOC Threat Hunting in Practice - Telecom Village
Social Engineering 101: The Four Psychological Backdoors to Scam Your Way into Anything - Social Engineering Community Village
Social Engineering 101: The Four Psychological Backdoors to Scam Your Way into Anything - Social Engineering Community Village
Social Engineering Community Village - Open Hours - Social Engineering Community Village
Social Engineering Community Village - Open Hours - Social Engineering Community Village
Social Engineering Community Village - Open Hours - Social Engineering Community Village
Social Engineering Community Village Party - Social Gatherings/Events
Social Engineering With Reel - Red Team Village
Software Defined Radios 101 - Introduction to RF Hacking - DEF CON Training
Software Defined Radios 101 - Introduction to RF Hacking - DEF CON Training
Software Quality in Electronic Voting - Voting Village
Sold Out - Agentic Threat Hunting: Building AI That Remembers What You Hunted - DEF CON Workshops
Sold Out - All About Stoopie InfoStealers: Malware Analysis for Understanding, Custom Coding for True Understanding! - DEF CON Workshops
Sold Out - Attacking Cloud APIs from the IoT Edge - DEF CON Workshops
Sold Out - AWS Cloud Security 101: From IAM Misconfigurations to Account Takeover - DEF CON Workshops
Sold Out - AWS Principal Threat Hunting: Behavioral Baseline for Malicious Activity - DEF CON Workshops
Sold Out - Battle-Tested Broadcasts: RF Insights From Ukraine - DEF CON Workshops
Sold Out - Building Agentic Reverse Engineering "Skills" - DEF CON Workshops
Sold Out - Building your own hardware hacking kit to Pentest Bluetooth, WIFI, and more. - DEF CON Workshops
Sold Out - CI/CD Weaponization: Build It, Deploy It, Own It - DEF CON Workshops
Sold Out - Creating Shellcode for Hackers - DEF CON Workshops
Sold Out - Detecting and Analyzing Memory Only Malware with Volatility 3 - DEF CON Workshops
Sold Out - Embedded Computing Tools for Wireless Hardware Hacking - DEF CON Workshops
Sold Out - Entra ID Persistence - Because Passwords Were Never the Problem - DEF CON Workshops
Sold Out - Explore the Windows instrumentation callback - DEF CON Workshops
Sold Out - From Prompt to PWN: Exploiting LLM Powered Web Applications with OWASP Techniques - DEF CON Workshops
Sold Out - HackTheCloud26: Chaining Cloud Misconfigurations to Compromise Infrastructure - DEF CON Workshops
Sold Out - Hands-on DuckyScript: An Introduction to HID Attack Tools with O.MG Devices - DEF CON Workshops
Sold Out - Hands-on IoT firmware extraction and flash forensics - DEF CON Workshops
Sold Out - Hecate: A Trivial UART Tool - DEF CON Workshops
Sold Out - ICS Hack 'n Track - DEF CON Workshops
Sold Out - Intro to Writing Windows Malware with Rust! - DEF CON Workshops
Sold Out - Introduction to Malware Analysis - DEF CON Workshops
Sold Out - Investigating and Responding to M365 account compromise on a shoestring: Living of the Land Incident Response - DEF CON Workshops
Sold Out - Learning to Hack Bluetooth Low Energy with BLE CTF - DEF CON Workshops
Sold Out - Learning to Reverse Engineer Compiled C as We Learn to Write It - DEF CON Workshops
Sold Out - Long Live Empire: A C2 Workshop for Modern Red Teaming - DEF CON Workshops
Sold Out - Malware Development 101 - From Zero to Hero: Adapt your payload to your environment - DEF CON Workshops
Sold Out - Offensive Packet Wizardry with Scapy - DEF CON Workshops
Sold Out - OT Systems: how to secure them in practice! - DEF CON Workshops
Sold Out - Pivot, Hunt, Publish: An Offline, Hands-On CTI Workshop for Blue Teams and Threat Researchers - DEF CON Workshops
Sold Out - Post-Quantum Cryptography (PQC) for Hackers - DEF CON Workshops
Sold Out - Purple Protocol: Adversary emulation for everyone - DEF CON Workshops
Sold Out - Purple Teaming Industrial Control Systems - DEF CON Workshops
Sold Out - Reaching Mythos: Hands-On Vulnerability Discovery with Local AI Models - DEF CON Workshops
Sold Out - Salesforce Apex Predator: Breaking Salesforce Sites - DEF CON Workshops
Sold Out - Solder, Detect, Listen: Build Your Own EMF Explorer - DEF CON Workshops
Sold Out - Step-by-Step Malware Development: Evading EDR from Loaders to the Kernel - DEF CON Workshops

Sold Out - Web Hacking 101 - DEF CON Workshops
Sold Out - Wi-Fight Club: I am Jack's Evil Twin - DEF CON Workshops
Sold Out - Words As Weapons: Breaking AI and Agents; Then Securing Them - DEF CON Workshops
Solving Modern Cybersecurity Problems with AI - DEF CON Training
Solving Modern Cybersecurity Problems with AI - DEF CON Training
Source of Truth: A Field Guide for Deep Technical Research - OWASP Foundation
Sovereign by Design, Vulnerable by Default - Policy @ DEF CON
SpaceCOP - Catch Me If You Can - Aerospace Village
SpaceCOP - Catch Me If You Can - Aerospace Village
SpaceCOP - Catch Me If You Can - Aerospace Village
SpaceCOP: Houston, We Have an Intrusion - Aerospace Village
Spotlight: Choose Your Own Adventure with InfoSecMap - OWASP Foundation
Spotlight: Choose Your Own Adventure with InfoSecMap - OWASP Foundation
Spotlight: Choose Your Own Adventure with InfoSecMap - OWASP Foundation
spyVspy 3: Rat Race - Contests
spyVspy 3: Rat Race - Contests
spyVspy 3: Rat Race - Contests
SR-71 Blackbird Badge Challenge - Aerospace Village
SR-71 Blackbird Badge Challenge - Aerospace Village
SR-71 Blackbird Badge Challenge - Aerospace Village
Stalking the Wily Hacker ... 40 years later - DEF CON Talks
StarPWN CTF - Contests
StarPWN CTF - Contests
Starting and Sustaining a Successful DEF CON Group presented by DC862 - DEF CON Groups
State Desync as a Weapon: Breaking Transactional Integrity in Payment Systems (ESP) - La Villa Community
Stay Sharp: Navigating Pen Testing and Bug Bounty in an AI-Driven World - The Diana Initiative
Stealing at the Speed of Light: The Anatomy of a Real Relay Attack tool - Car Hacking Village
Step Zero: Identifying the Quantum Attack Surface in Critical Infrastructure - Crypto & Privacy Village
Stigma is stupid: Let's talk about recovery, mental wellness, and hard stuff without making it awkward - The Diana Initiative
Stop Chasing Domain Admin: Designing Red Team Exercises That Matter - Red Team Village
Strategic AI Penetration: Mastering Offensive Techniques for LLMs - DEF CON Training
Strategic AI Penetration: Mastering Offensive Techniques for LLMs - DEF CON Training
Strategic Resistance: How a Global Network is Fighting the Spyware Industry - Policy @ DEF CON
Strengthening the CVE Ecosystem (Seating is limited to 50 Participants) - Policy @ DEF CON
Student-Run Cyber Clubs - Why They Matter & Digital Playgrounds - .EDU Community
Supertooth: Wideband Bluetooth Observation with a HackRF - Radio Frequency Village
Supply Chain Isn't Just Dependencies Anymore: Defending Developers, Tooling, and Builds - AppSec Village
Surprise Session - Check Hacker Tracker - Policy @ DEF CON
Tactical Advocacy: Panel & Peer Sessions with EFF - Policy @ DEF CON
Tag, You're It: Authorization Traps in AWS ABAC - Cloud Village
Tag, You're It: Physical Tracking Tech, Defense, and How to DIY Your Own - Recon Village
tAIrot Readings - Misc
Take Back Your Memories - Hackers.town
Taking on the Dark Fleet... in Cyberspace! - DEF CON Talks
Talkers Without Borders: Worldwide Free Speech without an Internet Connection - DEF CON Talks
Taming the Swarm: Hard Architectural Lessons from Building a Deterministic Agentic Web Pentesting System - DEF CON Talks
TBA - Blue Team Village
TCM Security Labs - Noob Community
TCM Security Labs - Noob Community
TCM Security Labs - Noob Community
Tech Reclaimers Update: A Year In, Building a Social Movement Away from Big Tech - Hackers.town
TEE.fail: Breaking Trusted Execution Environments via DDR5 Memory Bus Interposition - DEF CON Talks
TeleChallenge - Contests
TeleChallenge - Contests

TeleChallenge - Contests
Telecom Village CTF Awards Ceremony - Telecom Village
Telecom Village CTF Closure - Telecom Village
Telecom Village CTF Closure - Telecom Village
Telecom Village CTF - Telecom Village
Telecom Village Inauguration - Telecom Village
Telecom Village Open Forum: Talks & Workshops: Review, Highlights, and Key Learnings - Telecom Village
Telecom Village Open Forum: Talks & Workshops: Review, Highlights, and Key Learnings - Telecom Village
Telecom Village Tour - The Diana Initiative
Testing API Business Logic With AI Agents: What We Got Wrong First - Bug Bounty Village
Texas Incidents - How we broke the OMAP-L138 Trusted Execution Environment - DEF CON Talks
That's Not Your Agent: Why Zero Trust Can't Tell - AI Village
The 100-to-1 Problem: Securing the Non-Human Identity Perimeter - Cloud Village
The 2026 Pwnie Awards - DEF CON Talks
The Achaean project-Trojan development for noobs - Malware Village
The Agent Asked. We Allowed. Now What? - AppSec Village
The Agent Long Con: Tricking Agents Out of Their Data - Crypto & Privacy Village
The Agentic Free Pass: Does an Abliterated Backbone Make Agents Easier to Attack? - AI Village
The Agentic Free Pass: Does an Abliterated Backbone Make Agents Easier to Attack? - Middle Easterns & Africans in Cyber Security (MEACS)
The AI Analysis Train is Leaving the Station: ALL ABOARD!! - Malware Village
The Air Is Hostile: RF Trust Assumptions in Modern Security Systems - Red Team Village
The API Made Me Do It - Do Bad APIs Lead AI to Generate Vulnerable Code? - AppSec Village
The Authentic Operator: Social Engineering Through Natural Delivery - Red Team Village
The Autonomous Insider - Cloud Village
The Autonomous Security Loop - Cloud Village
The Autonomous SOC Blueprint: On-Premise ML & AI to Condense, Consolidate, Contextualize, Correlate & Co-Investigate Attack Chains Hiding in the Noise - Middle Easterns & Africans in Cyber Security (MEACS)
The best of three bad ideas? Ransomware taxes in lieu of bans or doing nothing - Policy @ DEF CON
The Black PhD Playbook: What No One Tells You - Blacks In Cyber Village
The Breach Is Over. The Exposure Is Not - Recon Village
The Call Stack Experience - AppSec Village
The Call Stack Experience - AppSec Village
The Camera Is Lying: RTSP Trust Failures in Modern Surveillance Systems - IoT Village
The Closing Window: Governing Agentic AI Security in a Post-Mythos World - Policy @ DEF CON
The Compiler Nobody Satisfactorily Tested: Supply-Chain Gaps in EV Charging Firmware - Car Hacking Village
The Compiler That Can't Read: Crashing Every 5G Phone With One Byte - DEF CON Talks
The Cost of Unverified Intelligence: AI and Accountability in Defense Operations - Blacks In Cyber Village
The Cum-Stained Precipice of Digital Redlining - Hackers.town
The CVE-Hunters Project: From Noobs to Researchers - La Villa Community
The Cyber Crystal Ball: The Annual Policy @ DEF CON Contingencies Survey - Policy @ DEF CON
The Dark Art of Alert Correlation: Extracting Attack Chains from Chaos - Middle Easterns & Africans in Cyber Security (MEACS)
The Death of Dicom - Biohacking Village
The DEF CON 34 Badge - DEF CON Talks
The Diana Initiative - Open time - The Diana Initiative
The Diana Initiative - Open time - The Diana Initiative
The Diana Initiative - Open time - The Diana Initiative
The Diana Initiative - Open time - The Diana Initiative
The Diana Initiative - Open time - The Diana Initiative
The Diana Initiative - Open time - The Diana Initiative
The Door Was Already Open - Physical Security Village
The Dots Do Matter: Gmail's Invisible Blindspot - AppSec Village
The EFF Benefit Poker Tournament - Contests
The Enclave is Lying to You: Breaking TEE Trust Boundaries Through Boot-Time State - DEF CON Talks

The Enshittified Internet and How We Can All Rewild the Internet - Hackers.town
 The Enshittified Internet and How We Can All Rewild the Internet - Hackers.town
 The Entropy Illusion: High-Speed Cracking on a Budget - Red Team Village
 The Front Lines Need Detection Engineers : Would You Like to Know More? - Noob Community
 The Future of Bug Bounty - Program Manager Perspective - Bug Bounty Village
 The Future of Payments: AI, Agentic Commerce and the Next Wave of Innovation - Payment Village
 The Ghost Key: Illusions of "Time Management" in TTLock Smart Locks - DEF CON Talks
 The Glass Perimeter: Systematic Bypasses in Biometric Frameworks and the Rise of Synthetic Identity - DEF CON Talks
 The Hard Part of ASM: Ownership Attribution - Recon Village
 The Hidden Cost of Agentic Connectivity - Cloud Village
 The Hidden Data Supply Chain: How a SaaS Platform Broadcast Credentials and Customer Identities - Middle Easterns & Africans in Cyber Security (MEACS)
 The impact of CTF Write-Ups - Noob Community
 The importance of Networking in Cybersecurity community - Noob Community
 The KEVOPS Sellout Pool Party II: Sponsored by Zyn - Social Gatherings/Events
 The Knox Box - A Brief History(Part II) - Lockpick Village
 The Liability Stack: When Code Becomes Conduct - Policy @ DEF CON
 The Modern Detection Engineer - Blue Team Village
 The National Fight Against ALPRs - Crypto & Privacy Village
 The New Horizons in Quantum and Space - Middle Easterns & Africans in Cyber Security (MEACS)
 The New Software Supply Chain Nobody is Securing: MCP - Cloud Village
 The Permanent Threat: Analyzing Aeternum's Blockchain-Based C2 Operations and Communications - Malware Village
 The Political economy of AI - Hackers.town
 The Polymorphic Agent: From Cross Agent Escalation to Just in Time Defense on Azure - Cloud Village
 The Protocol-Native Adversary: Full-Spectrum ICS Simulation via SiL - Red Team Village
 The Quantum Mechanic: Attacking all the clouds - Red Team Village
 The Republic is a Team Sport: Technology can Protect Elections, but the People must Protect Democracy - Voting Village
 The Ripple Effect: Inside Cloud-Scale Vulnerabilities in the Age of AI - Bug Bounty Village
 The Sandbox is a Suggestion: Deconstructing AI Agent Sandboxes - DEF CON Talks
 The Sherlock Holmes Social Engineering Playbook - Social Engineering Community Village
 The Silent Tunneler: A Real-World Incident Response Story - Malware Village
 The State of Decompiler Malware - Malware Village
 The State of DEF CON Groups - DEF CON Groups
 The Stream Is Dead, Long Live the Stream: How HTTP/2 Lets Dead Streams Keep Servers Working - DEF CON Talks
 The Subverted Hacker - Policy @ DEF CON
 The Unofficial DEF CON Shoot - Social Gatherings/Events
 The Voice Behind the Payload: Tracing AAVE Across Malware Artifacts - Blacks In Cyber Village
 There and Back Again - Voting Village
 There Is No Internet: Cross-Domain Recon of all 4.3 Billion IPv4s - Recon Village
 There's A Bug in My Boot! Finding Vulnerabilities in U-Boot - Packet Hacking Village
 Thin Client? Thin Crypto - Bypassing Full-Disk Encryption Across Three Major Thin Clients Vendors without Breaking a Cipher - DEF CON Talks
 This is a Test: Vibe Hacking LTE Cell Broadcast for Emergency Alert Injection - Radio Frequency Village
 This Message Was Sent by Microsoft: Turning Microsoft Apps into our Phishing Platform - DEF CON Talks
 This Wasn't AI Generated: Principles for Breaking Generative Watermarks - AI Village
 Thread Carefully - Embedded Systems Village
 Threat Actors: Gotta Catch 'Em All - Recon Village
 Threat Hunting 101: Beyond the Alerts - Blue Team Village
 Threat Hunting Explained Badly - Blue Team Village
 Threat Hunting in OT Networks - Using Hypothesis Based Methods - ICS Village
 Threat Intelligence in Real Life - Blue Team Village
 Threat Model your Career Workshop - The Diana Initiative
 Threat Modeling LLMs with PHANTOM-B - AppSec Village
 Threatmaxxing Your Stakeholders while Mogging Your Threat Actors: What is Cyber Threat Intel? - Noob Community
 ThreatPatrol: Visualising the Modern Threat Landscape - ICS Village

Threats in Space: The Dangerous Rise of GNSS Attacks - Telecom Village
Throw Out the Alphabet: Token-Based Markov Chains for Password Cracking - DEF CON Talks
Tin Foil Hat Contest - Contests
Tin Foil Hat Contest - Contests
Tin Foil Hat Contest - Contests
To Catch a Pseudoscientist - Biohacking Village
TokenMesh: Exposing Azure's Hidden Identity Attack Surface - Demo Labs
TokenMesh: Exposing Azure's Hidden Identity Attack Surface - Demo Labs
Tokens and PRT: Advanced Attacks and Persistence in Microsoft Entra ID - La Villa Community
Tokens and PRT: Advanced Attacks and Persistence in Microsoft Entra ID - Red Team Village
Tokens and PRT: Advanced Attacks and Persistence in Microsoft Entra ID - Cloud Village
Too Much "Slop" and Not Enough Soul: Why the AI Music Bubble is Leaking & Robots Shouldn't Replace Our Djs - Hackers.town
Total Recon: How We Discovered 1000s of open Agents in The Wild - Recon Village
Toxic BBQ - Social Gatherings/Events
Trace Labs L100: Search Party Basics - OSINT For Good Community
Trace Labs L150: Case Walkthrough - OSINT For Good Community
Tracelabs VM Installation Workshop - OSINT For Good Community
Tracking the Trackers: How We Took Over 36 Million GPS Devices Protecting Children and Vehicles - DEF CON Talks
TrackTheFugitive Contest - Recon Village
TrackTheFugitive Contest - Recon Village
Trajan: Cross-Platform CI/CD Security Scanner - Demo Labs
Trajan: Cross-Platform CI/CD Security Scanner - Demo Labs
Trans Meetup - Queercon Community
Trans Townhall - Queercon Community
Transformers: Dark Side of the Type - Weaponizing the Conversion Layer - DEF CON Talks
Travel Security: Viewing Risks Through the Eyes of a Hacker - Physical Security Village
Triage vs. Reality: Mobile Security Findings in Bug Bounty - Mobile Hacking Community
Trust Amplification in Enterprise AI Systems – Microsoft CoPilot Case Studies Enabling AI-Assisted Influence Operations - AI Village
Trust Fall: How Agentic AI Inherits Your Cloud's Worst IAM Habits - Cloud Village
Trust Me, Bro: A field guide to Windows Authenticode Abuse - Red Team Village
Trust No History: Why Every "Remembered" Interaction is a Potential Backdoor - AppSec Village
Trust the Basics, But Know Their Limits: Where Standard Cybersecurity Advice Falls Short - Crypto & Privacy Village
Trust the Cloud Pipeline, Lose the Kingdom - Cloud Village
Trust the Pipeline, Lose the Kingdom: Hands-On Cloud Native CI/CD Red Team - Red Team Village
Trusted Launcher, Untrusted Code: Weaponizing AppLaunch.exe to bypass SmartScreen and AppLocker - Red Team Village
Tu foco IoT nunca tuvo modelo de amenazas - La Villa Community
Turning Keys and Opening Doors: Leveraging AI Hype to Hack Everything - Red Team Village
Turning Recon Coverage into Bug Bounty Signal - Bug Bounty Village
Two NICs, Zero Trust: Pulling Apart a PAC Buried in Critical Infrastructure - ICS Village
UAIrT: Over The Air UART - IoT Village
Um, ACKtually - Contests
Unconference - Nix Vegas Community
Unlocking Vehicles by Brute-Forcing Rolling Code Systems - Car Hacking Village
Untechnical - Contests
Untechnical - Contests
Untechnical - Contests
Veilid- the Next Gen of privacy - DCNextGen
Very Pwned: Hacking Verifone's card machine three times in a row - DEF CON Talks
VETCON 2026 PARTY - Social Gatherings/Events
Vibe Check: Exploiting Developer Trust from Prompt Injections to Weaponized Repos - Malware Village
Vibe Coding Your Way to a Fully Functional Open-Source Intelligence Platform - Recon Village
Victim as a Service: Engaging with Trust-Based Scams Using AI - Payment Village
Village Greeting - Social Engineering Community Village

Visible Mending, repair and reinforce - Maker's Village
VoiceLock: Offline, Robust On-Device Speech Transcription - Demo Labs
VoiceLock: Offline, Robust On-Device Speech Transcription - Demo Labs
Voting Village Keynote - The Paper Chase - Voting Village
Voting Village Lab - Voting Village
Voting Village Lab - Voting Village
Voting Village Lab - Voting Village
Voting Village Tour - The Diana Initiative
VS: S-RAD (Satellite-Radio Analysis & Disruption) - DEF CON Training
VS: S-RAD (Satellite-Radio Analysis & Disruption) - DEF CON Training
Wall of Wallets Workshop (Intro to Wall of Wallets Challenge) - Payment Village
Wall of Wallets Workshop (Intro to Wall of Wallets Challenge) - Payment Village
Wand Protocol: Full-Chain Attack on an FDA-Listed Fertility Analyzer - Biohacking Village
Wanna Hack Space ? Why? Is it out of this world? - Noob Community
WarDriver Meetup - Radio Frequency Village
WASM Was Not the Boundary: Sandcastles, Not Sandboxes - DEF CON Talks
Watching Norway's Election - Voting Village
We Pwn Your Phone, We Pwn Your Vote (Demo and Panel) - Voting Village
Weaponization of Cellular Based IoT Technology – Leveraging Smart Devices to Gain a Foothold - IoT Village
Weaponizing CloudFormation: Privilege Escalation via Infrastructure as Code in AWS - Cloud Village
Weaponizing eBPF and XDP with Covert Triggered Reverse Shells - Demo Labs
Weaponizing eBPF and XDP with Covert Triggered Reverse Shells - Demo Labs
Weaponizing Uselessness: Breaking SMM with the Slowest Instruction Ever Written - DEF CON Talks
Web Hacking Bootcamp - Red Team Village
Web3 Security: Hacks, Scams, and Exploits - Cryptocurrency Village
Welcome Party at The Industrial - Social Gatherings/Events
Welcome to DEF CON 34! - DEF CON Talks
Welcome to OSINT4Good and Trace Labs - OSINT For Good Community
Welcome to the Voting Village - Voting Village
Welcome to your Airbnb, the key is under the mat -or- Alice and Bob with Padlocks - DCNextGen
What can those architecting agents learn from national security? - AI Village
What Election Security Researchers Need to Know About the DMCA - Voting Village
What Got You Here Won't Get You There: Security in the AI Era - Middle Easterns & Africans in Cyber Security (MEACS)
What is AI? Interactive, Unplugged Activity - AI Village
What is AI? Interactive, Unplugged Activity - AI Village
What is AI? - CodeBloom
What is AI? - CodeBloom
What is AI? - CodeBloom
What is AI? - CodeBloom
What is AI? - CodeBloom
What is the Right Balance of Rules for Defenders & Adversaries? Determining which dual-use model restrictions make sense and which only disarm defenders - DEF CON Talks
What Scammers Know That Social Engineers Don't: Three Techniques for Tough Cases - Social Engineering Community Village
What TEEs Do Not Hide: Residual Metadata Leakage in Confidential LLM Serving - Crypto & Privacy Village
What we learned from SATAN about the MYTH of Mythos - AI Village
What Your Coding Agent Did Last Night: Runtime Security for AI Coding Agents - AppSec Village
What's Behind the Curtain? Tearing Down AWS's AI Agent Runtime From the Inside - Cloud Village
When AI Finds Everything: Vulnerability Policy for the Coming Discovery Surge - Policy @ DEF CON
When Cash Runs on Windows: A Red Team Look at ATM Attack Surfaces - La Villa Community
When Machines Attack Machines: Detecting AI-Autonomous Cloud Compromise at NHI Scale - Cloud Village
When the Agent Lies: Why Neurosymbolic AI is the Security Layer Nobody is Building Yet - Blacks In Cyber Village
Where hackers find their people, and security finds its strength - Adversary Village
Where the Authorization Boundary Goes in Agent Workflows - Middle Easterns & Africans in Cyber Security (MEACS)
Who Owns Your Shack? Open Source, Amateur Radio, and the Software We Can't Afford to Lose - Ham Radio Village

Whose Agent Is It Anyway? Agency, Authorization, and Accountability in the Year of the AI Agent - Policy @ DEF CON
Whose PR Is It Anyway? - Nix Vegas Community
Whose PR Is It Anyway? - Nix Vegas Community
Whose Resource Is It Anyway? The Design Flaw That Breaks the IAM Permission Model - Cloud Village
Whose Slide Is It Anyway? - Social Gatherings/Events
Why Couldn't I See My Own Drone? Remote ID, ESP32s, and the Packet Trail to Friend or Foe - Packet Hacking Village
Why Mandatory Age Verification Keeps Us All Less Safe - Misc
Why Signals Still Matter: Amateur Radio in the Age of Cell Phones - Ham Radio Village
Wi-Fi Self Defense & Hacker Hunting & For Beginners - IoT Village
Wi-Fi Self Defense & Hacker Hunting & For Beginners - IoT Village
Wi-Fi Self Defense & Hacker Hunting & For Beginners - IoT Village
WiFi Shuriken: A New Architecture For High Performance Scanning - Radio Frequency Village
Wiring the Harness: Orchestrating Frontier Models for Vulnerability Hunting at Scale - Packet Hacking Village
Witchcraft Solver: Automated Oday Discovery in Stripped Binaries - DEF CON Talks
Wolfmasking: Teaching Everyday Defenders to Think Like Social Engineers - Social Engineering Community Village
Women Loving Women Meetup - Queercon Community
Women, gender non-conforming and non-binary meetup with The Diana Initiative - Social Gatherings/Events
Work Session: Binary Code - CodeBloom
Work Session: Binary Code - CodeBloom
Work Session: Ciphers - CodeBloom
Work Session: Ciphers - CodeBloom
Work Session: Ciphers - CodeBloom
Work Session: Ciphers - CodeBloom
Work Session: Ciphers - CodeBloom
Work Session: Ciphers - CodeBloom
Workshop Before the SIEM Blinks: How AI Memory Turns Alerts into Intelligence - La Villa Community
Wrestling with a Python: Escaping Copilot Studio's AI-Guarded Sandbox - DEF CON Talks
Write Once, Shell Everywhere: Turning Arbitrary File Writes into RCE - Bug Bounty Village
Writing Production-Grade Exploits in go-exploit - Red Team Village
Writing to Shadow Stacks - DEF CON Talks
X-Ray Your Agents: Pentesting MCPs, Skills, and the Plugin Supply Chain - Demo Labs
X-Ray Your Agents: Pentesting MCPs, Skills, and the Plugin Supply Chain - Demo Labs
xEndity: IoT Firmware Analysis & Digital Twin Platform - Demo Labs
xEndity: IoT Firmware Analysis & Digital Twin Platform - Demo Labs
Yes, I froze an SNES for science - Game Hacking Village
Yes, it runs Doom: over the air gaming on a bladeRF SDR - Radio Frequency Village
Yet Another Walking Dead of Active Directory - Adversary Village
Yoga - The Diana Initiative
Yoga - The Diana Initiative
You Can't Block My C2 — It's Your Google Calendar - Red Team Village
You Can't Opt Out: The Invisible Surveillance in Your Walls, Pockets, and Lives - IoT Village
You Hold the Helm: Agentic LLM Workflows for Malware Reversing - Malware Village
You're Hired... Maybe: Inside Cybersecurity Hiring in 2026 - Blue Team Village
You're Probably Using FPE Wrong - Crypto & Privacy Village
You've Got Mail (That Was Meant For No One) - DEF CON Talks
You're Invited to Get Hacked: Real-World Exploits in Modern Invitation Systems - Bug Bounty Village
Your Bank Thinks I'm You: A Complete Kill Chain Against Mobile Banking Security - DEF CON Talks
Your Infrastructure Is a DAG: Manage It With Nix - Nix Vegas Community
Your Lives are in Another Struct: Breaking Memory Hacks with Field Relocation - Game Hacking Village
Your OpSec Is Showing - Recon Village
Your OTP Never Arrived: Attacking the Trust Boundary Where SMS Meets the Internet - DEF CON Talks
Your Packets Are Showing: Hybrid Quantum ML for Passive OS Fingerprinting - DEF CON Talks
Your Passkeys Won't Save You: Conditional Access Bypass via Auth-Method Downgrade - Red Team Village
Your SaaS Is My Foothold: Weaponizing Shadow SaaS for Initial Access and Persistence - AppSec Village
Your WAF Blocked Us, That Was The Exploit - Remote Agent Takeover via Cloudflare, Sentry and Claude Zero-Day for

[data exfil - DEF CON Talks](#)

[Zealot: An Autonomous Cloud Offensive Multi-Agent System - Demo Labs](#)

[Zealot: An Autonomous Cloud Offensive Multi-Agent System - Demo Labs](#)

[Zero Day Hire: Can You Spot the Spy? - Social Engineering Community Village](#)

[Zero Day Hire: Can You Spot the Spy? - Social Engineering Community Village](#)

[Zero Signal: Operating Where Defenders Can't See - Red Team Village](#)

[Zero Trust Kubernetes Security: Preventing Real World Container Attacks - AppSec Village](#)

[Zero-Cloud Threat Modeling: Vector Embedding Architectures for Automated Vulnerability Detection - Demo Labs](#)

[Zero-Cloud Threat Modeling: Vector Embedding Architectures for Automated Vulnerability Detection - Demo Labs](#)

[Zero-Day Provisioning: Chaining TP-Link ZTP Vulnerabilities for Infiltrating Networks - DEF CON Talks](#)

[Zero-Knowledge Unsaflok: The Unsaflok Saga Continues - Physical Security Village](#)

Creator/Village Talk List

[.EDU Community](#)

PDT Times	Title	speaker
Friday		
11:00 - 11:59	Cracking the Cybersecurity Career Code with the Cy . . .	Shavvon "TheSiren" Cintro . . .
12:00 - 12:59	Student-Run Cyber Clubs - Why They Matter & Digita . . .	Steven "Stengo" Ngo
13:00 - 13:59	ScamBusters: Turning Undergrads into Threat Hunter . . .	Angela "BlondeTechie" Ram . . .
14:00 - 14:59	Hacking Education - Teaching Offensive Cyber Scien . . .	Dave "Rebelcadet" Ortiz
17:00 - 17:59	.edu Community Mixer	

[Return to Index](#)

Adversary Village

Location: LVCCW Level 1 Hall 2 602 (Adversary Village) - [Map](#)

Home Page: <https://adversaryvillage.org>

Sched Page: <https://adversaryvillage.org/adversary-events/DEFCON-34/schedule/>

PDT Times	Title	speaker
Friday		
11:30 - 11:59	Haetae: An Agent to Takedown North Korean C2 Serve . . .	Mauro Eldritch,Nelson Raf . . .
12:00 - 12:30	Yet Another Walking Dead of Active Directory	Nikos "nickvourd" Vourdas
13:15 - 13:59	From threat-intel to tested defense, the adversary . . .	Cheryl Biswas,Adam Pennin . . .
14:00 - 14:45	6 years of Adversary Village! Keeping up with the . . .	Abhijith "Abx" B R,Bryson . . .
14:45 - 15:15	SEND: Teaching Machines to Lie to Defenders	Yi Ting Shen,Ariz Soriano
15:15 - 15:45	Hey Adversary, I've Got a Human EDR Bypass for Y . . .	Daniel Isler
17:15 - 17:59	Where hackers find their people, and security find . . .	Seeyew Mo,Ashley S,Tatian . . .
Saturday		
10:30 - 10:59	Emulating the "Identity-First" Threat Actor: A . . .	Samet Can Tasci,Mehmet Ö . . .
10:00 - 10:30	MCPwned: How Exposed AI Agents Became the Internet . . .	Eli Woodward
13:30 - 13:59	Field Notes on Offensive Agents: Reusability, Reli . . .	Dominika Pietrzak,Ibai Ca . . .
14:00 - 14:30	Microsoft and Amazon are my Favorite C2 Providers	Robert Pimentel
Sunday		
11:00 - 11:30	Beyond the Hype: The Real Role of Red Teams in an . . .	Michael Leibowitz,Niranja . . .

[Return to Index](#)

Aerospace Village

Location: LVCCW Level 1 Hall 2 700 (Aerospace Village) - [Map](#)

Home Page: <https://aerospacevillage.org/>

PDT Times	Title	speaker
Friday		
10:00 - 17:59	MOUSE Runner & Flappy Drone	
10:00 - 17:59	Mission: Compromised - Hacking a Satellite from th . . .	
10:00 - 17:59	Nebula Showdown: Space Systems Security CTF Advent . . .	
10:00 - 17:59	SR-71 Blackbird Badge Challenge	
10:00 - 17:59	Satellites Under Attack: Hands-On Satellite Securi . . .	
10:00 - 17:59	SpaceCOP - Catch Me If You Can	
10:00 - 17:59	Flight Simulator/EFB	
10:00 - 17:59	Drone Hacking Workshop	
10:00 - 17:59	Drone Hacking Choose your Own Adventure	
10:00 - 17:59	DCNextGen - Space Grand Challenge - SatHack: The M . . .	
10:00 - 17:59	DCNextGen - RIC-1: ELT Localization Exercise - N3V . . .	
10:00 - 17:59	DCNextGen - Bricks in the Air	
10:00 - 17:59	Bricks in the Air	
10:00 - 17:59	Aviation ISAC Cybersecurity Challenge	
10:00 - 17:59	Aerospace Ecosystem Resilience Innovation Environm . . .	
10:00 - 17:59	ARINC 664 CTF Challenge	
10:00 - 10:30	Hacking Electronic Conspicuity Devices -or- Making . . .	Ken Munroe
12:45 - 13:30	Aerospace Cybersecurity Student Research Spotlight . . .	Clara Davis,Dylan Gururaj . . .
12:00 - 12:45	Aerospace Cybersecurity Student Research Spotlight . . .	Sean McConoughey,Samuil N . . .
13:30 - 13:59	Hacking Airplanes at the NTSB	David Case,Jonathan Xue
15:00 - 15:30	Drones, Detectors, and the Kill Chain	Greg Albrecht
15:30 - 15:59	Cleared for Takeoff: Debunking “Uncertifiable” . . .	Katie Fejer
Saturday		
10:00 - 17:59	ARINC 664 CTF Challenge	
10:00 - 17:59	Flight Simulator/EFB	
10:00 - 17:59	Drone Hacking Workshop	
10:00 - 17:59	Drone Hacking Choose your Own Adventure	
10:00 - 17:59	DCNextGen - Space Grand Challenge - SatHack: The M . . .	
10:00 - 17:59	DCNextGen - RIC-1: ELT Localization Exercise - N3V . . .	
10:00 - 17:59	DCNextGen - Bricks in the Air	
10:00 - 17:59	Bricks in the Air	
10:00 - 17:59	Aviation ISAC Cybersecurity Challenge	
10:00 - 17:59	Aerospace Ecosystem Resilience Innovation Environm . . .	
10:00 - 17:59	Mission: Compromised - Hacking a Satellite from th . . .	
10:00 - 17:59	Nebula Showdown: Space Systems Security CTF Advent . . .	
10:00 - 17:59	SR-71 Blackbird Badge Challenge	

PDT Times	Title	speaker
10:00 - 17:59	Satellites Under Attack: Hands-On Satellite Securi . . .	
10:00 - 17:59	SpaceCOP - Catch Me If You Can	
10:00 - 17:59	MOUSE Runner & Flappy Drone	
11:30 - 11:59	So You Want to Work in Aircraft Cyber? Here's what . . .	Matt Gaffney,Marcie Wise
11:00 - 11:30	Security Analysis of Open-Source Software Used in . . .	Roe Idan
14:00 - 14:30	Racing PX4: Memory Safety and Timing Vulnerabiliti . . .	Nefeli Georgilas
14:30 - 14:59	Hacking AFDX or Not; A Primer for Flight Control S . . .	Andrew Tierney,Adam Bromi . . .
17:00 - 17:30	Behind the Badge: SAOV3 and Open Sourcing the Aero . . .	Adam Batori,Kevin Colley, . . .
17:30 - 17:59	SpaceCOP: Houston, We Have an Intrusion	Brandon Bailey

Sunday

10:00 - 13:59	Mission: Compromised - Hacking a Satellite from th . . .
10:00 - 13:59	Nebula Showdown: Space Systems Security CTF Advent . . .
10:00 - 13:59	SR-71 Blackbird Badge Challenge
10:00 - 13:59	Satellites Under Attack: Hands-On Satellite Securi . . .
10:00 - 13:59	SpaceCOP - Catch Me If You Can
10:00 - 13:59	MOUSE Runner & Flappy Drone
10:00 - 13:59	Flight Simulator/EFB
10:00 - 13:59	Drone Hacking Workshop
10:00 - 13:59	Drone Hacking Choose your Own Adventure
10:00 - 13:59	DCNextGen - Space Grand Challenge - SatHack: The M . . .
10:00 - 13:59	DCNextGen - RIC-1: ELT Localization Exercise - N3V . . .
10:00 - 13:59	ARINC 664 CTF Challenge
10:00 - 13:59	DCNextGen - Bricks in the Air
10:00 - 13:59	Aerospace Ecosystem Resilience Innovation Environm . . .
10:00 - 13:59	Bricks in the Air
10:00 - 13:59	Aviation ISAC Cybersecurity Challenge

[Return to Index](#)

AI Village

Location: LVCCW Level 1 Hall 2 603 (AI Village) - [Map](#)

Home Page: <https://aivillage.org/>

PDT Times	Title	speaker
Friday		
10:00 - 17:59	AI Village: Village Open	
10:00 - 10:30	AI Village: Opening Remarks	
10:00 - 17:59	Cyber Mirage: Realtime Deepfake Demos	Brandon Kovacs
10:00 - 17:59	Poster Presentations	
14:00 - 14:59	Fooing Coding Agents for Fun and Profit	Matt Galligan,Jack Cable
15:00 - 15:59	Pwning the Internet of Agents: Zero-Click Backdoor . . .	João Maria Campos Donato . . .
16:00 - 16:59	Bruce's Fireside Chat	Bruce Schneier
16:30 - 16:59	Minimize Harm, Maximize Defense: How Anthropic Nav . . .	Curt Barnard
Saturday		
10:00 - 17:59	Cyber Mirage: Realtime Deepfake Demos	Brandon Kovacs
10:00 - 17:59	Poster Presentations	
10:00 - 17:59	AI Village: Village Open	
11:00 - 11:59	What is AI? Interactive, Unplugged Activity	Sam Mosley
12:00 - 12:45	This Wasn't AI Generated: Principles for Breaking . . .	Thomas Mason,Tahseen Rabb . . .
12:00 - 12:45	AgentBreaker: A blind spot detector for your codin . . .	Aditi Narasimhan,Farzaan . . .
14:00 - 14:59	The Agentic Free Pass: Does an Abliterated Backbon . . .	Karol Piekarski,Nishith S . . .
14:00 - 14:30	What we learned from SATAN about the MYTH of Myths . . .	Jeff Crume
14:30 - 14:59	That's Not Your Agent: Why Zero Trust Can't Tell	Krity Kharbanda,Emma Yuan . . .
15:00 - 15:59	What can those architecting agents learn from nati . . .	David C Eight
16:00 - 16:59	MeshLens: Security Profiling at Scale	Vipul Ujawane,Jigar Bhavs . . .
16:30 - 16:59	Trust Amplification in Enterprise AI Systems – M . . .	Tobias Diehl
17:30 - 17:59	SADF: A Taxonomy and Evaluation Framework for Agen . . .	Julie Brunias
Sunday		
10:00 - 13:59	Cyber Mirage: Realtime Deepfake Demos	Brandon Kovacs
10:00 - 13:59	AI Village: Village Open	
10:30 - 10:59	Scaling Adversary Emulation with Autonomous Agents	Daniel Fabien
10:00 - 10:30	A Billion-User Blast Radius: Owning ChatGPT's Se . . .	Simcha Kosman
11:00 - 11:59	What is AI? Interactive, Unplugged Activity	Sam Mosley
12:30 - 12:59	AI Village: Closing Remarks	
12:00 - 12:30	Pwning Agentic Browsers with PleaseFix: A New Vuln . . .	Stav Cohen
12:30 - 12:59	Leveraging Large Language Models for Policy, Regul . . .	Dr. Deepti Gupta,Sai Sith . . .

[Return to Index](#)

AppSec Village

Location: LVCCW Level 1 Hall 2 604 (Appsec Village) - [Map](#)

Home Page: <https://www.appsecvillage.com/>

Sched Page: <https://www.appsecvillage.com/events/dc-2026>

PDT Times	Title	speaker
Friday		
10:15 - 11:15	Pentesting made easy - Keeping sessions alive with ...	Kai Glauber,Matthias Göh ...
10:30 - 12:30	Burp, But Yours: Hands-On Extension and Bambda Dev ...	Hannah L
10:30 - 10:59	The Dots Do Matter: Gmail's Invisible Blindspot	Keren Elazari
11:30 - 12:30	Aegis of the Vulnerable: A Unified Pipeline for AI ...	Can Oztas
11:10 - 11:40	Pickled and Exposed: RCE in AI Serving Frameworks	Iggy
11:50 - 12:20	A Billion-User Blast Radius: Owning ChatGPT's Secu ...	Simcha Kosman
11:00 - 12:59	Cards Against Vulnerabilities	Patrick Smyth
11:00 - 12:59	The Call Stack Experience	Victoria Keeler
11:00 - 12:59	Clash of Prompts: The World's First Prompt Battle ...	
11:00 - 12:59	Hack the Duck Store	Gwendal Mognier,Samantha ...
12:45 - 13:45	Drogonsec: SAST + SCA + Secrets + IaC in one open- ...	Filipi Pires
12:30 - 12:59	Container Escapes Are Not Magic. Here Is How They ...	Advait Patel
13:30 - 13:59	Agentic Chaos - What 86K+ Agent Codebases Reveal A ...	Bar Kaduri,Lidan
13:00 - 14:59	Cards Against Vulnerabilities	Patrick Smyth
13:00 - 14:59	AI Pentesting Trivia Showdown	Andy Dennis,Bill Reyor
13:00 - 14:59	Factory Floor MVP Incident Response Challenge	
13:00 - 14:59	AppSec Quiz Gauntlet: Spot the Vulnerability	Avek Kolech
14:00 - 14:59	Farsight: Turning OSINT into Actionable Attack Sur ...	Arif,Sai Vernekar,Seedon ...
14:30 - 16:59	Container Escapes 101	some-natalie
14:50 - 15:20	GeoHacking: from memory corruption RCE to cross te ...	Michal Kamensky
14:10 - 14:40	from_pretrained() to from_pwned(): Breaking Huggin ...	Yotam Perkal
15:15 - 16:15	IDEViewer - Securing Developer Workstations from I ...	securient
15:30 - 15:59	Zero Trust Kubernetes Security: Preventing Real Wo ...	Janakiram Meka
15:00 - 16:59	Cards Against Vulnerabilities	Patrick Smyth
15:00 - 16:59	AI Pentesting Trivia Showdown	Andy Dennis,Bill Reyor
15:00 - 16:59	SBOM Find the Flaws	Dmitry Raidman
15:00 - 16:59	NPM Imposters - The malware detection card game	Mackenzie
16:30 - 17:30	Rebuilding Code Security with Signal, Speed and AI	Derek C.,Shasheen Bandodk ...
16:50 - 17:20	Most threat modeling artifacts don't help coding a ...	Meitar Ronen
16:10 - 16:40	Man-in-the-Browser: Hijacking Javascript APIs for ...	Aarav Juneja
17:30 - 17:59	Trust No History: Why Every "Remembered" Interacti ...	Barno Kaharova,Rico Komen ...
Saturday		
10:15 - 11:15	In Untrust We Can Trust: Enforcing Trust Boundarie ...	Yariv Tal
10:15 - 12:59	Prompt Injection: Attacking and Defending AI-Power ...	Mohammed Ilyas Ahmed
10:30 - 10:59	Building Hackbots	Jason "jhaddix" Haddix

PDT Times	Title	speaker
11:30 - 12:30	Precogly: Open-Source Threat Modeling for the AI-C . . .	Vikramaditya Narayan
11:50 - 12:20	Past the Bouncer: The Limits of CSP, Eleven Years . . .	Pedro Fortuna
11:10 - 11:40	What Your Coding Agent Did Last Night: Runtime Sec . . .	Inga Cherny
11:00 - 12:59	Code Invaders: Stop The Insecure Code	Mackenzie
11:00 - 12:59	Pentester vs AI: Race The Machine, In Real Life	Gwendal Mognier,Samantha . . .
11:00 - 12:59	Cards Against Vulnerabilities	Patrick Smyth
11:00 - 12:59	SBOM Find the Flaws	Dmitry Raidman
12:45 - 13:45	OWASP FinBot CTF: Hands-On Agentic AI Threats	Helen Oakley,saikishu
12:30 - 12:59	Threat Modeling LLMs with PHANTOM-B	Adam Shostack
13:15 - 15:59	Supply Chain Isn't Just Dependencies Anymore: De . . .	Tanya "SheHacksPurple" Ja . . .
13:30 - 13:59	How Shadow APIs Become an Attacker's Free Pass Int . . .	Emma Yuan Fang,Krity
13:00 - 14:59	Code Invaders: Stop The Insecure Code	Mackenzie
13:00 - 14:59	AppSec Quiz Gauntlet: Spot the Vulnerability	Avek Kolech
13:00 - 14:59	AI Pentesting Trivia Showdown	Andy Dennis,Bill Reyor
13:00 - 14:59	Factory Floor MVP Incident Response Challenge	
14:00 - 14:59	OWASP AIBOM Generator	Dmitry Raidman,Helen Oakl . . .
14:50 - 15:20	Pattern, Graph, Prompt: What Happens When You Laye . . .	Mudita Khurana
14:10 - 14:40	Every ride you take - Hacking a City's Public Tr . . .	Ignacio Navarro
15:15 - 16:15	Proactive Malicious Package Defense	Darren Meyer
15:30 - 15:59	How Malicious AI Skills Hijack Your Agents	Jenn Gile
15:00 - 16:59	SBOM Find the Flaws	Dmitry Raidman
15:00 - 16:59	AppSec Quiz Gauntlet: Spot the Vulnerability	Avek Kolech
15:00 - 16:59	AI Pentesting Trivia Showdown	Andy Dennis,William Reyor
15:00 - 16:59	The Call Stack Experience	Victoria Keeler
16:30 - 17:30	Your SaaS Is My Foothold: Weaponizing Shadow SaaS . . .	Jordan Bonagura
16:15 - 17:59	Code to Cloud: Secure Modern Applications Using Op . . .	Mackenzie
16:10 - 16:40	The API Made Me Do It - Do Bad APIs Lead AI to Gen . . .	Yariv Tal
16:50 - 17:20	No Jailbreak Required: Pwning AI Agents Through th . . .	Helen Oakley,saikishu
17:30 - 17:59	From Prompts to Production: Discovering Exposed PI . . .	Samantha Pearlstein
Sunday		
10:15 - 11:15	ROP for the Web: Smuggling XSS, SQLi, and Web Shel . . .	alevsk
10:15 - 12:59	Introduction to AI-Enhanced Threat Modeling Worksh . . .	Robert Hurlbut
10:30 - 10:59	From commit to compromise: securing the full pipel . . .	Filipi Pires
11:30 - 12:30	search_vulns: Navigating the Fragmented Landscape . . .	Dustin Born,Matthias Göh . . .
11:10 - 11:40	Extending Shared Threat Models with the Applicatio . . .	J Fridley
11:50 - 12:20	Finding Bugs Is Easy, Patching Isn't: Build Your O . . .	Mohan Kumar,Naveen
11:00 - 12:59	Clash of Prompts: The World's First Prompt Battle . . .	Darren McNelis,Jerome Rob . . .
11:00 - 12:59	AppSec Quiz Gauntlet: Spot the Vulnerability	Avek Kolech
11:00 - 12:59	SBOM Find the Flaws	Dmitry Raidman
11:00 - 12:59	NPM Imposters - The malware detection card game	Mackenzie
12:45 - 13:45	The Agent Asked. We Allowed. Now What?	Liran Lavi,Sarit Yerushal . . .

Biohacking Village

Location: LVCCW Level 1 Hall 1 408 (Biohacking Village) - [Map](#)

Home Page: <https://www.villageb.io/>

Sched Page: <https://www.villageb.io/Labs>

PDT Times	Title	speaker
Friday		
10:00 - 17:59	Embedded & Shredded: Advanced Embedded System Hack . . .	
10:00 - 17:59	Biohacking Device Lab	
10:00 - 10:45	Four Newbies Vs. An Insulin Pump. How Hard Can It . . .	Birgitte Jordal,Julia Kuc . . .
10:00 - 10:45	Counting the Dead in the Digital Siege: Detection . . .	Jorge Acevedo Canabal,Sco . . .
11:30 - 11:59	Human in the Loop or Human Out of Luck?	Christine Von Raesfeld
15:45 - 16:30	Snap, Crackle, Popped: How to manage a massive cyb . . .	David Nathans
16:30 - 17:15	Lights Out and Last Call: A Drunken Tabletop on Me . . .	Courtney McCarty
17:30 - 17:59	Hacking Hearts by Reverse Engineering Pacemaker Fi . . .	Marie Moe,Shayan Alinejad . . .
Saturday		
10:00 - 17:59	Embedded & Shredded: Advanced Embedded System Hack . . .	
10:00 - 17:59	Biohacking Device Lab	
10:00 - 10:30	To Catch a Pseudoscientist	James Utley PhD
10:30 - 10:59	The Death of Dicom	Michael "v3ga" Aguilar
13:00 - 13:30	Safe, Secure, and Effective: What Static Behavior . . .	Andrew Hendela
15:00 - 15:30	AIRGAP BREACHED: Monitoring the Ancestral Payload . . .	David J. Castillo-Cornejo
15:30 - 15:59	DarkSyringe: Automated poisoning of Clinical AI As . . .	Francesco Costa
Sunday		
10:00 - 13:59	Embedded & Shredded: Advanced Embedded System Hack . . .	
10:00 - 13:59	Biohacking Device Lab	
10:30 - 10:59	Wand Protocol: Full-Chain Attack on an FDA-Listed . . .	Gigi Xiaoqing Liu

[Return to Index](#)

Blacks In Cyber Village

Location: LVCCW Level 3 W322-W324 (BIC Village) - [Map](#)

Home Page: <https://www.blacksincyberconf.com/bic-village>

Sched Page: <https://www.blacksincyberconf.com/bic-village>

PDT Times	Title	speaker
Friday		
10:00 - 10:55	Return of the Defender: Using AI to Strike Back Ag . . .	Levone Campbell
11:00 - 11:55	The Black PhD Playbook: What No One Tells You	Dr. Fatou Sankare,Dr. Xav . . .
12:00 - 12:25	When the Agent Lies: Why Neurosymbolic AI is the S . . .	Maureese Williams
12:30 - 12:55	Prompt Injection Detection in Large Language Model . . .	Yasmin Eady
13:00 - 13:55	CTRL the Chaos: When AI Controls Critical Infrastr . . .	Nykolas Muldrow
14:00 - 14:55	Agents on Alert: Building an AI-Powered Threat Inv . . .	Samson Adewale
15:00 - 15:25	The Cost of Unverified Intelligence: AI and Accoun . . .	Kayrene Woods
15:30 - 15:55	Configuring Your Favorite Platforms to Prioritize . . .	Malachi Walker,Anthony Jo . . .
16:00 - 17:30	KaliGPT Vibe-Ethical Hacking Session	Timothy E. Bates
Saturday		
10:00 - 10:55	Being Black While Hacking: The Unofficial Survival . . .	Dr. Louis DeWeaver III
11:00 - 11:55	Cyber Gamechangers: Women Who Lead, Secure, and In . . .	Nikkia Henderson,Arielle . . .
12:00 - 12:25	Root Access: An APT Analysis of Systemic Gatekeepi . . .	Dr. Hassan Karim
12:30 - 12:55	The Voice Behind the Payload: Tracing AAVE Across . . .	Brett Alexander Tolbert
13:00 - 13:55	Bias is a Bug: Why Inequality is a Cybersecurity V . . .	Dr. Fatou Sankare
14:00 - 14:55	Exploring Security Features in the Armv8-M Archite . . .	Ian Harris,Jacob Gutierre . . .
15:00 - 15:55	ChronoRoot: Time-Traveling Through Kernel Trust Bo . . .	Ahmeen Muhammad,Sydney Jo . . .
16:00 - 16:30	Improving Security Vulnerability Descriptions usin . . .	Kenechukwu Nwodo
16:30 - 16:59	[Virtual] National Service Panel - CTU,BIC,MCPA	Carmeshia Miller,Tiffany . . .
Sunday		
10:00 - 10:59	From Practitioner to Principal: Building a Cyberse . . .	Tyrone E. Wilson
11:00 - 11:30	Quantum Computing The Game Changer You Can t Ignor . . .	Danielle Eason
12:00 - 12:20	Monocultures Are Vulnerabilities: Representation a . . .	Ruben Stephen
13:00 - 13:59	DeNISTifying Technology: Paradigm Shifting To Quan . . .	Aisha Berry

[Return to Index](#)

Blue Team Village

Location: LVCCW Level 2 W213-217 (Blue Team Village) - [Map](#)

Home Page: <https://blueteamvillage.org/>

Sched Page: <https://btv-dc34.sessionize.com/schedule/day/20260807>

PDT Times	Title	speaker
Friday		
10:00 - 10:59	Incident Response 101: Preparing Before the Hack, . . .	Joshua Morgan
11:00 - 11:59	Cyber Threat Intelligence 101: From Foundations to . . .	Carlo Anez Mazurco
12:00 - 12:59	Digital Forensics 101	Sarthak Taneja
13:15 - 14:15	TBA	
14:30 - 15:30	Building Project Obsidian: Designing the Blue Team . . .	Carlo Anez Mazurco,Chris . . .
15:45 - 16:45	The Modern Detection Engineer	Alex Hurtado,Chase Phelps . . .
17:00 - 17:59	Cloudy with a Chance of Venting: Managing Supply C . . .	Cassandra (muteki) Young, . . .
Saturday		
10:00 - 10:59	AI for Defenders 101	Anirudh Pratap Singh,Neha . . .
11:00 - 11:59	Threat Hunting 101: Beyond the Alerts	Kainu ~
12:00 - 12:59	Cloud Forensics 101 : Ghost in the logs	Cassandra (muteki) Young, . . .
13:15 - 14:15	Threat Intelligence in Real Life	Ashley Sequeira,Julian Zo . . .
14:30 - 15:30	AI Security: Hype, Hacks, and the Future of Defens . . .	Karan Dwivedi,Thomas Rocc . . .
15:45 - 16:45	Threat Hunting Explained Badly	Allison Gallo,Brian Bask . . .
17:00 - 17:59	Incident Response in 2026	Chriss Hansen,K Singh,Lev . . .
Sunday		
11:00 - 11:59	You're Hired... Maybe: Inside Cybersecurity Hiring . . .	George Scheibe,Neha Gauta . . .

[Return to Index](#)

Bug Bounty Village

Location: LVCCW Level 2 W206-207 (Bug Bounty Village) - [Map](#)

Home Page: <https://bugbountydefcon.com/>

Sched Page: <https://www.bugbountydefcon.com/agenda-2026>

PDT Times	Title	speaker
Friday		
10:00 - 10:59	The Future of Bug Bounty - Program Manager Perspec . . .	Jai Kumar Sharma,Catherin . . .
10:00 - 10:30	Click Me: Turning URI Links into Bug Bounty RCE's	Tobias Diehl
10:30 - 11:30	Hacking IDE Extensions - VSCode Workshop	Nick "7urb01" Copi
11:30 - 11:59	Make Money Hacking AI	Joey Melo,Edward Morris
11:00 - 11:30	The Ripple Effect: Inside Cloud-Scale Vulnerabilit . . .	Albin Vattakattu,Ryan Nol . . .
11:30 - 12:30	Hackbots	Jason "jhaddix" Haddix,Ry . . .
12:00 - 12:30	Write Once, Shell Everywhere: Turning Arbitrary Fi . . .	Bruno Mendes,Rafael Casti . . .
12:30 - 12:59	Beyond Theoretical Risk: How Cache Poisoning Escal . . .	Glendon Chong
12:30 - 13:30	AI Hacking Workshop: Bug Bounty Edition	Ben "NahamSec" Sadeghipou . . .
14:00 - 14:30	AI Nightmare: Hacking at 0-Hour	Pedro "drop" Paniago
14:00 - 14:59	Navigating AI-Assisted Submissions	Tony Lee,Michael Skelton, . . .
15:30 - 15:59	Hunting for Cryptographic Ghosts: A Bug Hunter's . . .	Samet Berk Simsek,Ahmet F . . .
15:00 - 15:30	Cache Key Injection: Smuggling Poison Through the . . .	Alex Brumen
15:00 - 15:59	a [REDACTED] history of this hobby	Chris "flyingtoasters" Ho
16:00 - 16:59	Hacking Human-in-the-Loop systems	Inti "securinti" De Ceuke
17:00 - 17:59	Beyond Normalization: The Expanding Unicode Attack . . .	Ryan "ryancbarnett" Barne . . .
Saturday		
10:00 - 10:30	Shadow Webhooks: Hunting for Dangling Event Listen . . .	Samet Can Tasci,Mehmet Ö . . .
10:30 - 10:59	Testing API Business Logic With AI Agents: What We . . .	Samantha Pearlstein
10:00 - 10:45	Turning Recon Coverage into Bug Bounty Signal	Radu Stefan Voloaga
10:45 - 11:30	You're Invited to Get Hacked: Real-World Exploit . . .	Ali "logic-breaker" Kabee . . .
11:30 - 12:30	De-Sloppify: Your AI Needs a Proxy	Emile "TheSyttten" Fugulin . . .
12:00 - 12:30	Killing AI Slop: A Multi-Model Orchestration Frame . . .	Armaan Pathan
12:30 - 12:59	Eating Our Own Dogfood: Running a Bug Bounty Progr . . .	Shrimant Subhash More,Mar . . .

PDT Times	Title	speaker
12:30 - 13:30	Better Bug Hunting on AI Products: A VRP Lead's ...	John Kotheimer
14:00 - 14:30	Exfil Everything: A Year of Stealing Data from AI ...	Ads Dawson, Mike "TakSec" ...
14:30 - 15:59	Bots, Bounties, and Bullshit: An Honest Panel on A ...	Ben "NahamSec" Sadeghipou ...
16:00 - 17:59	Burp, But Yours: Hands-On Extension and Bambda Dev ...	Hannah L
Sunday		
10:30 - 10:59	Slop Spotting, Using Rules to Detect AI Slop for B ...	Katie Paxton-Fear, Max vo ...
10:00 - 10:30	Skill Issue: A Recon Story	Ryan Bonner
10:00 - 10:30	AI Cuts Both Ways: Using AI to Find More Bugs, and ...	Ciarán "monke" Cotter
11:30 - 11:59	Automated Discovery of Prompt Injection Vulnerabil ...	Bogdan Stelee, Arnav Garg
11:00 - 11:30	Full Disclosure, Full Screen: [Informative] The St ...	Abhinav "TweetsFromPanda" ...
11:30 - 11:59	Heavy Metal and Hidden Secrets: A Five-Year Retros ...	Ariel "arl_rose" Garcia
12:00 - 12:59	How We Built Xenoptic: A Walkthrough of Design, In ...	Adham Elmosalamy, Ahmed At ...
13:45 - 14:15	Bug Bounty Village Closing Ceremony	Bug Bounty Village Staff

[Return to Index](#)

Call Center Village

Location: LVCCW Level 2 W218 (Call Center Village) - [Map](#)

Home Page: <https://www.callcentervillage.com/>

Sched Page: <https://www.callcentervillage.com/events>

PDT Times	Title	speaker
Friday		
10:00 - 17:59	Call Center Village - Open	
15:00 - 15:59	An Intrusion in the Living Room is now an internat . . .	D3adA55
Saturday		
10:00 - 17:59	Call Center Village - Open	
Sunday		
10:00 - 13:59	Call Center Village - Open	

[Return to Index](#)

Car Hacking Village

Location: LVCCW Level 1 Hall 2 701 (Car Hacking Village) - [Map](#)

Home Page: <https://www.carhackingvillage.com/>

Sched Page: <https://www.carhackingvillage.com/defcon-34-talks>

PDT Times	Title	speaker
Friday		
10:00 - 16:59	Bomb Bot Challenge	
10:00 - 17:59	Car Hacking Village Open	
Saturday		
10:00 - 17:59	Car Hacking Village Open	
10:00 - 16:59	Bomb Bot Challenge	
15:30 - 15:59	The Compiler Nobody Satisfactorily Tested: Supply- . . .	Kangwon Lee
16:00 - 16:30	Free IP, Free Chaos: DHCP-Assisted Flooding Againsts . . .	Yehyeong Lee
Sunday		
10:00 - 13:59	Car Hacking Village Open	
10:30 - 10:59	Unlocking Vehicles by Brute-Forcing Rolling Code S . . .	Danilo Erazo
11:30 - 11:59	Stealing at the Speed of Light: The Anatomy of a R . . .	Robbie Galfrin

[Return to Index](#)

Cloud Village

Location: LVCCW Level 3 W311-W313 (Cloud Village) - [Map](#)

Home Page: <https://cloud-village.org/>

Sched Page: <https://www.cloud-village.org/dc34>

PDT Times	Title	speaker
Friday		
10:50 - 11:30	Tokens and PRT: Advanced Attacks and Persistence i . . .	Elzer Pineda,Jose Rivas
10:10 - 10:50	New AWS IAM Attack Paths and the Framework to Expl . . .	Seth Art
10:00 - 10:10	Opening Talk	Jayesh Singh Chauhan
11:00 - 12:59	Weaponizing CloudFormation: Privilege Escalation v . . .	Samanta Aranda
11:00 - 12:59	Governing the Firehose: Writing Custom OPA Policie . . .	Ram "n2r"
11:30 - 12:10	From Pipeline to Cloud Control	Saksham Agrawal
12:50 - 13:20	PurpleLoop: Closing the Loop Between Detection Rul . . .	Ariz Soriano
12:10 - 12:50	Security at Machine Speed: How Autonomous AI Agent . . .	Pujita Sahni,Geoff Sweet
13:30 - 15:30	Cloudy with a Chance of Breaches: Hands-On AWS Thr . . .	Kyle Hubbard
13:30 - 14:30	The Autonomous Security Loop	Jeremy Schiefer,Lawton Pi . . .
13:20 - 13:59	The Hidden Cost of Agentic Connectivity	David Fiser,Amy McMahon
14:00 - 14:30	Nebula - 5 years, still kicking *aaS	Bleon "gl4ssesbo1" Proko
14:30 - 15:10	Citizen Developers Can't Defend What They Built: S . . .	
15:10 - 15:30	Go with the Flow: Riding GCP Dataflow Shadow Depen . . .	Gil Weizman,Tamir Yehuda
15:30 - 16:10	The Polymorphic Agent: From Cross Agent Escalation . . .	Muskan Tomar
16:00 - 17:59	Cirro: Extending Your Azure Graph Beyond Identitie . . .	Leron Gray
16:00 - 17:59	From Dashboard to Exploit: Weaponizing and Winning . . .	Mackenzie Jackson
16:10 - 16:50	The New Software Supply Chain Nobody is Securing: . . .	
16:50 - 17:30	Trust Fall: How Agentic AI Inherits Your Cloud's W . . .	Aravind Sreekanth Pallavo . . .
Saturday		
10:00 - 10:40	Bashing CloudShells for mining, networking, exfil . . .	Jenko "edleft" Hwong,Chri . . .
10:40 - 11:20	Ghost Records: Automating Dangling DNS & Subdomain . . .	Jai Kumar Sharma,Tom McCa . . .
11:00 - 12:59	Patch Me If You Can: Hands-On Network Threat Defen . . .	Don Bogert
11:00 - 12:59	From Findings to Remediations: Open Source Cloud S . . .	Toni de la Fuente,Amit Sh . . .
11:20 - 11:59	Trust the Cloud Pipeline, Lose the Kingdom	Shane Young
12:20 - 12:59	Pinchy Gets Played: How We Red-Teamed AI Agents Be . . .	Doron Kapah
12:00 - 12:20	Whose Resource Is It Anyway? The Design Flaw That . . .	Moshe Berntsein
13:30 - 14:30	Breaking AWS Bedrock: Novel Attack Techniques Agai . . .	Tal Peleg,Maya Parizer
13:30 - 14:30	Fix It, Snooze It, or Ignore It? Cloud Security De . . .	Mackenzie Jackson

PDT Times	Title	speaker
13:30 - 14:10	What's Behind the Curtain? Tearing Down AWS's AI A . . .	Dan Gansel
13:00 - 13:30	Minimal by Design: Building Hardened Near-Zero-CVE . . .	Kyle Quest,Ritvik Arya
14:10 - 14:50	Autonomous Offense vs. Autonomous Defense: Who's W . . .	
14:50 - 15:20	cloud-auth: a provider-agnostic CLI for cross-clou . . .	Aniruddha Biyani
15:20 - 15:59	A New Hope for SSRF: Exploiting Credential Relay f . . .	Marios Gyftos,Chrysostomo . . .
16:00 - 17:59	OCIGuana - A vulnerable-by-design OCI lab	Eli Shparaga
16:00 - 16:59	Securing the AI Stack and Hunting Across Clouds	Bryant Pickford
16:40 - 17:20	Key Rotation Won't Save You: Hunting Workload Iden . . .	Jie Wu
16:00 - 16:40	The 100-to-1 Problem: Securing the Non-Human Ident . . .	
Sunday		
10:40 - 11:20	When Machines Attack Machines: Detecting AI-Autono . . .	Gowthamaraj Rajendran
10:00 - 10:40	Tag, You're It: Authorization Traps in AWS ABAC	Itay Saraf
11:00 - 12:59	The Autonomous Insider	Naveen Reddy Pogalla,Hari . . .
11:50 - 12:30	Foxveil: Cloud-Native Loader Tradecraft on Cloudfl . . .	Shani Kurtzberg,Zohar Bub . . .
11:20 - 11:50	Breaking the Oracle: Building an Offensive Securit . . .	Scott Weston
12:30 - 13:10	Root-as-a-Service: The Hidden Runtime of Azure AI . . .	Shani Peled
13:10 - 13:30	Closing Talk	Jayesh Singh Chauhan

[Return to Index](#)

CodeBloom

Home Page: <https://codebloom.org/>

PDT Times	Title	speaker
Friday		
10:00 - 10:59	Game Time: Loops	
11:00 - 11:59	Work Session: Ciphers	
12:00 - 12:59	Game Time: Input, Output, and Variables	
13:00 - 13:59	What is AI?	Sam Mosley
14:00 - 14:59	Work Session: Ciphers	
15:00 - 15:59	Game Time: Input, Output, and Variables	
16:00 - 16:59	What is AI?	Sam Mosley
17:00 - 17:59	Work Session: Binary Code	
Saturday		
10:00 - 10:59	Game Time: Loops	
11:00 - 11:59	Work Session: Ciphers	
12:00 - 12:59	Game Time: Input, Output, and Variables	
13:00 - 13:59	What is AI?	Sam Mosley
14:00 - 14:59	Work Session: Ciphers	
15:00 - 15:59	Game Time: Input, Output, and Variables	
16:00 - 16:59	What is AI?	Sam Mosley
17:00 - 17:59	Work Session: Binary Code	
Sunday		
10:00 - 10:59	Game Time: Loops	
11:00 - 11:59	Work Session: Ciphers	
12:00 - 12:59	Game Time: Input, Output, and Variables	
13:00 - 13:59	What is AI?	Sam Mosley
14:00 - 14:59	Work Session: Ciphers	

[Return to Index](#)

Contests

Home Page: <https://defcon.outel.org/dcwp/dc34/activities/c/>

PDT Times	Title	speaker
Wednesday		
22:00 - 22:59	Raitlin's Challenge	
Friday		
09:00 - 11:59	SEC Vishing Competition (SEVCV)	
10:00 - 12:59	Aw, man...pages!	
10:00 - 17:59	5N4CK3Y	
10:00 - 17:59	DC's Next Top Threat Model	
10:00 - 17:59	Untechnical	
10:00 - 17:59	DEF CON Scavenger Hunt	
10:00 - 17:59	Darknet-NG	
10:00 - 17:59	Crack Me If You Can 2026	
10:00 - 17:59	TeleChallenge	
10:00 - 17:59	HackFortress	
10:00 - 17:59	?Cube	
10:00 - 17:59	\$unLight Sh4d0w5	
10:00 - 10:59	Octopus Game - Opening Ceremony	
10:00 - 12:59	Octopus Game Opens and Pre-registration Check-In A . . .	
10:00 - 17:59	Octopus Game - Booth Open	
10:00 - 17:59	Beer Chilling Contraption Contest	
10:00 - 17:59	Cryptid Hunt	
10:00 - 17:59	HSPACE: AI Battlegrounds	
10:00 - 17:59	spyVspy 3: Rat Race	
10:00 - 17:59	Hacker Games	
10:00 - 17:59	PhreakMe	
10:00 - 17:59	Game Hacking Village CTF	
10:00 - 17:59	Kubernetes CTF	
10:00 - 17:59	Hac-Man	
10:00 - 17:59	Crack the Core	
10:00 - 17:59	Cyber Deck Competition	
10:00 - 17:59	Pinball High Score Contest	
10:00 - 17:59	Code Cadaver: Break Every System. Save Your Friend . . .	
10:00 - 17:59	PWN UR H0M3 - DDoS CTF	
10:00 - 17:59	Real7y Overrun - Contest running	
10:00 - 17:59	Tin Foil Hat Contest	
10:00 - 17:59	CMD+CTRL Cyber Range: DarkMoney	
10:00 - 17:59	DEF CON CTF: Benevolent Bureau of Birds	
10:00 - 17:59	AI Village Plays Pokemon: DEFCON Edition	Nick Ashworth

PDT Times	Title	speaker
10:00 - 17:59	AI Village - Hal CTF	
10:00 - 11:59	StarPWN CTF	
10:00 - 16:59	Car Hacking Village CTF	
10:30 - 11:30	OWASP CTF: Getting started & welcome	Diego Cotel,Chris "dafin" . . .
10:00 - 17:59	OWASP CTF	
10:00 - 11:59	Blue Team Village CTF - Project Obsidian	
10:00 - 17:59	Escalation Desk CTF	
10:00 - 17:59	DEF CON Groups Sticker Contest	
10:00 - 17:59	DEF CON Groups Backdoors & Breaches	Tim Doerges,Seth Benning
10:00 - 23:59	Apex Park (Cloud Village CTF)	
10:00 - 10:59	Bug Bounty Village CTF - Open	
10:00 - 17:59	Hacking GRC Contest	
11:00 - 17:59	Radio Frequency Capture the Flag	
11:00 - 11:59	Radio Frequency Capture the Flag	
12:00 - 12:59	BIC Village Capture the Flag (CTF)	
12:00 - 14:59	The EFF Benefit Poker Tournament	Cindy Cohn,Jennifer Grani . . .
13:00 - 10:59	Octopus Game - Walk-In Registration (Pre-Registrat . . .	
13:30 - 14:59	Octopus Game - Booth Battle #1: The Front Man's Wa . . .	
13:00 - 17:59	Locktopus - Open Qualifying	
13:00 - 15:59	SEC Vishing Competition (SECVVC)	
13:00 - 14:59	Pub Quiz at DEF CON	
14:00 - 14:59	DEF CON Beard and Mustache Contest	
16:00 - 17:59	Um, ACKtually	
17:00 - 17:59	Octopus Game - Booth Battle #2: The Midnight "Braw . . .	
19:00 - 20:59	AI Art Battle	
Saturday		
10:00 - 11:59	Hack3r Runw@y v8.0	
10:00 - 17:59	5N4CK3Y	
10:00 - 17:59	DC's Next Top Threat Model	
10:00 - 17:59	Untechnical	
10:00 - 17:59	DEF CON Scavenger Hunt	
10:00 - 17:59	Darknet-NG	
10:00 - 17:59	Crack Me If You Can 2026	
10:00 - 17:59	TeleChallenge	
10:00 - 17:59	HackFortress	
10:00 - 17:59	?Cube	
10:00 - 17:59	\$unL1ght Sh4d0w5	
10:00 - 17:59	Octopus Game - Booth Open	
10:00 - 17:59	Beer Chilling Contraption Contest	
10:00 - 17:59	Cryptid Hunt	
10:00 - 17:59	HSPACE: AI Battlegrounds	
10:00 - 17:59	spyVspy 3: Rat Race	
10:00 - 17:59	Hacker Games	

PDT Times	Title	speaker
10:00 - 17:59	PhreakMe	
10:00 - 17:59	Game Hacking Village CTF	
10:00 - 17:59	Kubernetes CTF	
10:00 - 17:59	Hac-Man	
10:00 - 17:59	Crack the Core	
10:00 - 17:59	Cyber Deck Competition	
10:00 - 17:59	Pinball High Score Contest	
10:00 - 17:59	Code Cadaver: Break Every System. Save Your Friend . . .	
10:00 - 17:59	PWN UR H0M3 - DDoS CTF	
10:00 - 17:59	Real7y Overrun - Contest running	
10:00 - 17:59	Tin Foil Hat Contest	
10:00 - 17:59	CMD+CTRL Cyber Range: DarkMoney	
10:00 - 17:59	Radio Frequency Capture the Flag	
10:00 - 17:59	DEF CON CTF: Benevolent Bureau of Birds	
10:00 - 17:59	AI Village Plays Pokemon: DEFCON Edition	Nick Ashworth
10:00 - 17:59	AI Village - Hal CTF	
10:00 - 11:59	StarPWN CTF	
10:00 - 16:59	Car Hacking Village CTF	
10:00 - 17:59	OWASP CTF	
10:00 - 11:59	Blue Team Village CTF - Project Obsidian	
10:00 - 17:59	Escalation Desk CTF	
10:00 - 17:59	DEF CON Groups Backdoors & Breaches	Tim Doerges,Seth Benning
10:00 - 17:59	DEF CON Groups Sticker Contest	
10:00 - 23:59	Apex Park (Cloud Village CTF)	
10:00 - 10:59	Bug Bounty Village CTF - Open	
10:00 - 17:59	Hacking GRC Contest	
12:00 - 14:59	Dozier Drill Tournament	
12:00 - 15:59	Global OSINT Search Party CTF – DEF CON 34 Editi . . .	
12:00 - 12:59	BIC Village Capture the Flag (CTF)	
13:00 - 14:59	Crash and Compile - Stage Competition	
13:00 - 10:59	Octopus Game - Walk-In Registration (Pre-Registrat . . .	
13:00 - 13:59	Octopus Game - Booth Battle #3: The Marbles Match	
13:00 - 13:59	Locktopus - Semi Finals	
15:00 - 15:59	Locktopus - Final Championship	
15:30 - 17:30	Locktopus Challenge Finals	
17:00 - 17:59	Octopus Game - The Final Booth Battle	
18:00 - 20:59	EFF Tech Trivia	
22:00 - 23:59	Feet Feud (Hacker Family Feud)	
Sunday		
10:00 - 11:59	5N4CK3Y	
10:00 - 11:59	DC's Next Top Threat Model	
10:00 - 11:59	Untechnical	
10:00 - 11:59	DEF CON Scavenger Hunt	

PDT Times	Title	speaker
10:00 - 11:59	Darknet-NG	
10:00 - 11:59	Crack Me If You Can 2026	
10:00 - 11:59	TeleChallenge	
10:00 - 11:59	HackFortress	
10:00 - 11:59	?Cube	
10:00 - 11:59	\$unLight Sh4d0w5	
10:00 - 11:59	Beer Chilling Contraption Contest	
10:00 - 11:59	Cryptid Hunt	
10:00 - 11:59	HSPACE: AI Battlegrounds	
10:00 - 11:59	spyVspy 3: Rat Race	
10:00 - 11:59	Hacker Games	
10:00 - 11:59	PhreakMe	
10:00 - 11:59	Game Hacking Village CTF Q&A / Walkthroughs	
10:00 - 10:30	Game Hacking Village CTF awards ceremony	
10:00 - 11:59	Kubernetes CTF	
10:00 - 11:59	Hac-Man	
10:00 - 11:59	Crack the Core	
10:00 - 11:59	Cyber Deck Competition	
10:00 - 11:59	Pinball High Score Contest	
10:00 - 13:59	Code Cadaver: Break Every System. Save Your Friend . . .	
10:00 - 11:59	PWN UR H0M3 - DDoS CTF	
10:00 - 11:59	Real7y Overrun - Contest running	
10:00 - 11:59	Tin Foil Hat Contest	
10:00 - 12:59	CMD+CTRL Cyber Range: DarkMoney	
10:00 - 10:59	Radio Frequency Capture the Flag	
10:00 - 11:59	DEF CON CTF: Benevolent Bureau of Birds	
10:00 - 13:59	AI Village Plays Pokemon: DEFCON Edition	Nick Ashworth
10:00 - 13:59	AI Village - Hal CTF	
10:00 - 11:59	Car Hacking Village CTF	
10:00 - 11:59	Escalation Desk CTF	
10:00 - 10:30	Contest Awards	
10:00 - 11:59	Hacking GRC Contest	
12:00 - 12:59	PWN UR H0M3 DDoS CTF Winner Announcements	
13:00 - 13:45	Bug Bounty Village CTF Awards	Bug Bounty Village Staff

[Return to Index](#)

Crypto & Privacy Village

Location: LVCCW Level 1 Hall 1 401 (Crypto & Privacy Village) - [Map](#)

Home Page: <https://cryptovillage.org/>

Sched Page: <https://cryptovillage.org/cpv-13/>

PDT Times	Title	speaker
Friday		
10:30 - 10:59	What TEEs Do Not Hide: Residual Metadata Leakage i . . .	Anup Swamy Veena
13:00 - 13:30	Trust the Basics, But Know Their Limits: Where Sta . . .	Yael Grauer
14:30 - 14:59	You're Probably Using FPE Wrong	Leslie Gutschow
14:00 - 14:30	Inside the Guts of Ransomware	Ashley Hiram Muñoz
15:45 - 16:30	Step Zero: Identifying the Quantum Attack Surface . . .	Dr. Katrina Rosseini,Dr. . . .
16:30 - 17:15	Crypto Is Fine. The Code Is Not: Real-World Crypto . . .	Diptendu Kar
17:15 - 17:59	2026 is the New 2016: Relearning the Lessons from . . .	Anthony Hendricks
Saturday		
11:00 - 11:59	Gold Bug: Puzzle Panel with Friends	CPV Gold Bug Team 2026,TB . . .
14:00 - 14:59	Forget FIPS: An Analysis of Russian and Chinese Cr . . .	Infocalypse
15:00 - 15:59	The Agent Long Con: Tricking Agents Out of Their D . . .	Patrick Walsh
16:00 - 16:30	Quantum-Ready or Not: What 1,000 Codebases Reveal . . .	Dr. Zulfikar Ramzan
17:00 - 17:59	The National Fight Against ALPRs	Freddy Martinez,Sarah
Sunday		
11:00 - 11:30	Cove: Compositional and Verifiable Confidential Co . . .	Stephanie,Robin,Erika Lee

[Return to Index](#)

Cryptocurrency Village

Location: LVCCW Level 1 Hall 2 702 (Cryptocurrency Village) - [Map](#)

Home Page: <https://www.cryptocurrencyvillage.cc/>

Sched Page: <https://www.cryptocurrencyvillage.cc/village/>

PDT Times	Title	speaker
Friday		
11:00 - 11:59	Cryptocurrency Opening Keynote	Michael "MsvB" Schloh,Par . . .
14:00 - 14:59	Cryptohack Badge Hacking	Do Truong Giang "FSNaix", . . .
17:00 - 17:59	Blockchain defense, stablecoin attacks, and Web3 O . . .	Dinmukhammed "Celestial" . . .
Saturday		
10:00 - 10:59	Web3 Security: Hacks, Scams, and Exploits	Philip "AlephNull" Werlau . . .
13:00 - 13:59	Evading LLM Detection	Hanley Shun,Cong Zhang,. . .
16:00 - 16:59	Breaking Ciphers and Zero-Knowledge Proofs	Luke Szramowski,Freeman S . . .
Sunday		
11:00 - 11:59	Cryptocurrency Closing Keynote	Chelsea Button,Param "P7R . . .

[Return to Index](#)

Data Duplication Village

Location: LVCCW Level 2 W203 (Data Duplication Village) - [Map](#)

Home Page: <https://dcddv.org/>

Sched Page: <https://dcddv.org/dc34-talks-schedule>

PDT Times	Title	speaker
Thursday		
16:00 - 18:59	DDV open and accepting drives for duplication	
Friday		
10:00 - 17:59	DDV open and accepting drives for duplication	
11:00 - 11:59	Drive Stats: 14 years of hard drive failure rates	Stephanie Doyle
13:00 - 13:30	Forcing Physical Interlocks into Data Transit and . . .	Mehmet Önder Key,Temel D . . .
Saturday		
10:00 - 17:59	DDV open and accepting drives for duplication	
11:00 - 11:59	Poison the Well: RAG Attacks Against the Hacking C . . .	Omer Farooq
12:15 - 12:45	Forcing Physical Interlocks into Data Transit and . . .	Mehmet Önder Key,Temel D . . .
13:00 - 13:59	Drive Stats: 14 years of hard drive failure rates	Stephanie Doyle
Sunday		
10:00 - 10:59	Last chance to pick up drives at the DDV	

[Return to Index](#)

DCNextGen

Home Page: <https://dcnextgen.org/>

PDT Times	Title	speaker
Friday		
10:30 - 11:30	DCNextGen Opening Ceremonies	BiaSciLab
12:00 - 12:45	Cryptographer Recruitment: Crack the Substitution . . .	Bradán Lane
13:00 - 13:30	Locked Out? Let's Fix That: An Introduction to the . . .	Greg Anderson
14:00 - 14:45	Hack the Airwaves – Embedded Wireless for Next-G . . .	Adventures of Illya
15:00 - 15:45	Level Up - Could your Gaming Talents be Perfect fo . . .	The Hacking Games
16:00 - 16:30	Veilid- the Next Gen of privacy	medus4
17:00 - 17:45	Welcome to your Airbnb, the key is under the mat - . . .	Gilgamesh
Saturday		
10:00 - 10:30	Intro to Scratch	N3rd H3Rder
11:00 - 11:45	Meshpocalypse: Building Your Own Off-Grid Hacker N . . .	Adventures of Illya
12:00 - 12:30	AI and You: Staying Safe in the AI Era	Zoe Reid+Echo419
13:00 - 14:15	Hacker Culture 101	medus4
15:00 - 15:40	AMA with EFF	EFF
16:00 - 16:40	3D Printing: Data, Discretion, and Design	Evan
17:00 - 17:45	Objectively Awesome Robots: A Hands-On Introductio . . .	4ng3lhacker
Sunday		
10:00 - 10:59	Cloud Village CTF: Three Azure Warmups	Cloud Village
12:00 - 12:30	A Teen BadgeMaker's Journey of Creation	World Machine
13:30 - 14:30	DCNextGen Closing Ceremonies	BiaSciLab

[Return to Index](#)

DEF CON Groups

PDT Times	Title	speaker
Thursday		
10:00 - 17:59	DEF CON Groups (DCG)	
Friday		
10:00 - 17:59	DEF CON Groups (DCG)	
11:30 - 11:59	Starting and Sustaining a Successful DEF CON Group . . .	C\$,Joe Folk,Christopher " . . .
13:30 - 14:30	Darknet Diaries Meet & Greet with Jack Rhysider	Jack Rhysider
Saturday		
10:00 - 17:59	DEF CON Groups (DCG)	
11:00 - 11:30	Building a Hacker Haven: The Long Game of Growing . . .	Ryan Zagrodnik,Allie Zagr . . .
13:00 - 13:30	Building a Strong Community Culture presented by D . . .	Edna Jonsson,Dustin
Sunday		
10:00 - 10:30	Lessons Learned from Building a New DEF CON Group . . .	Cliff "GritsnGravy" Fried . . .
10:00 - 13:59	DEF CON Groups (DCG)	
11:00 - 11:30	The State of DEF CON Groups	Alethe Denis,Magen Wu

[Return to Index](#)

DEF CON Talks

Home Page: <https://defcon.outel.org/dcwp/dc34/activities/dctalks/>

PDT Times	Title	speaker
Friday		
10:00 - 11:59	Car Hacking Village Scavenger Hunt Contest	
10:30 - 10:59	The DEF CON 34 Badge	Andrew 'bunnie' Huang
10:00 - 10:30	Welcome to DEF CON 34!	Jeff "The Dark Tangent" M...
10:00 - 10:30	Breaking the Ethereum Phone: From BootROM to Walle...	Guanxing Wen
10:30 - 11:30	Breaking Local AI Runtimes: Exploiting llama.cpp a...	Ofek Itach,Vladimir "G1ND...
10:00 - 10:59	From square root to /root: escalating privileges i...	Ron Ben Yizhak
10:00 - 10:30	Weaponizing Uselessness: Breaking SMM with the Slo...	Christopher "xoreaxeaxeax...
10:30 - 11:30	Reflections on Disregarding Trust (Weaponizing CDP...	Gregory "lumberhack" Disn...
10:00 - 10:59	Texas Incidents - How we broke the OMAP-L138 Trust...	Carlo Meijer,Wouter Boksl...
11:00 - 11:59	The 2026 Pwnie Awards	Ian Roos,Mark Trumpbour
11:30 - 12:30	Crashing the Party: Pwning Control-Flow Integrity...	Marcos "h3xduck" Bajo,Rit...
11:00 - 11:59	Sliding into the Flight Deck's DMs: Practical Me...	Martin "MasorX" Strohmeie...
11:30 - 12:30	A Provider for the MOFia - Distributed Post-Ex Cap...	Steven Flores
11:00 - 11:59	Keychained Melody - Grabbing the Keys to the iCloud...	Alex Radocea,Jaron Bradle...
12:00 - 12:30	Your Packets Are Showing: Hybrid Quantum ML for Pa...	Daniel Justice,Jae Sung K...
12:30 - 13:30	Fireside Chat with Gen. Paul Nakasone	Paul Nakasone,Jeff "The D...
12:30 - 13:30	BTR Reforged: Weaponizing Defender's Remediation D...	Jiří Vinopal
12:30 - 12:59	DC101	Nikita Kronenberg,Michael...
12:00 - 12:30	Shopping Is The Attack: A Decade Of E-Commerce Sca...	Yaniv "PSYMAG" Menasherov
12:30 - 12:59	Hacking the Government: How Two Researchers Turned...	Robert "ProXy" Kruczek,Ka...
12:30 - 13:30	Patch Gap to Mobile Renderer RCE: Pwning Samsung I...	Hrvoje Mišetić,Jamie Hi...
12:00 - 12:59	Can AI do novel security research? Meet the HTTP T...	James "albinowax" Kettle
13:30 - 14:59	What is the Right Balance of Rules for Defenders &...	Emanuel Gawrieh,Jason Cli...
13:30 - 14:30	Breaking into Amazon lockers by any means necessar...	Martin Vigo
13:00 - 13:59	LGTM: Bypassing an LLM Build Gate When Prompt Inje...	Aviv Donenfeld
13:30 - 14:30	Plug And Pwn: Weaponizing Windows PnP Auto-Install	Alejandro "Oxedh" Hernand...
13:00 - 13:59	Bring-Your-Own-EDR - Breaking Windows Process Prot...	Shahak Morag
14:30 - 15:30	WASM Was Not the Boundary: Sandcastles, Not Sandbo...	Saar Pearl,Vladimir "G1ND...
14:00 - 14:59	8 Out of 10 Banks in Belgium HATE This One Weird e...	James "Acorn221" Arnott
14:30 - 14:59	Lowering the Orbit: Exploiting Satellite Protocols...	Romel "r0r0x" Marin
14:00 - 14:59	Lessons from a decade of building whistleblower te...	Trevor Timm,redshiftzero
15:00 - 15:59	The Stream Is Dead, Long Live the Stream: How HTTP...	Gal Bar Nahum
15:30 - 16:30	Your Bank Thinks I'm You: A Complete Kill Chain Ag...	Xavier "@xaferima" Riofri...
15:00 - 15:59	Hacking the Hackers who Hack Hackers: Supply-Chain...	Assaf Morag
15:00 - 15:30	Pwning Rekordbox: Unauthenticated filesystem acces...	Christopher "TRIODE" Le
15:30 - 16:30	Riding for Free - Breaking Public Transport RFID a...	Aidan "luu176" Nakache
15:00 - 15:59	Data Tomb Raider: Raiding Modern AI Vaults with Le...	Dolev Taler,Mark Vaitsman

PDT Times	Title	speaker
16:00 - 16:59	The Sandbox is a Suggestion: Deconstructing AI Age . . .	Elad Meged
16:30 - 17:30	noRecognition: Could a pattern on your clothing fo . . .	Bill "hevnsnt" Swearingen
16:00 - 16:59	Hacking the EOD Bot: How I Learned to Stop Worryin . . .	Patrick "gigstorm" Kiley, . . .
16:30 - 17:30	CloudBashing: Exploiting free CloudShells for mini . . .	Jenko "edleft" Hwong,Chri . . .
16:00 - 16:59	Certified Re-Pwned: escalating all the way up	Daniel Monzon,Eric Labrad . . .
17:00 - 17:59	Hacking AI	Bruce Schneier
17:30 - 17:59	Breaking Hardware CFI with Sigreturn	Omri "beta_b0t" Ben Bassa . . .
17:00 - 17:59	One Chain to Own Them All — Breaking AI Infrastr . . .	Ji'an "azraelxuemo" Zhou, . . .
17:30 - 17:59	You've Got Mail (That Was Meant For No One)	Cøry "interpunkt" Solov . . .
17:00 - 17:59	Gotta Catch 'Em All: How To Capture 3.5 Billion Wh . . .	Maximilian Guenther,Gabri . . .
Saturday		
10:00 - 11:59	Car Hacking Village Scavenger Hunt Contest	
10:00 - 10:59	The Ghost Key: Illusions of "Time Management" in T . . .	Yang Liu,Zhenghan Wang
10:00 - 10:30	Memory Laundering via Metal: What EDR Can't See on . . .	Hxr1
10:30 - 11:30	Harvest Now, Decrypt Later: Practical Attacks on P . . .	Aleksandr Krasnov
10:00 - 10:59	From Wind Farm to CHP Plant: The Untold Story of L . . .	Marcin Dudek
10:00 - 10:30	No Socket, No Privs, No Problem: Weaponizing OCI R . . .	David "davidrxchester" Ro . . .
10:30 - 11:30	Root From Kilometers Away: Ubiquiti AirMax RCE	Federico Kirschbaum,Gasto . . .
10:00 - 10:59	Identity Crisis: Novel Vulnerabilities leading to . . .	Shai Laron
11:00 - 11:59	Tracking the Trackers: How We Took Over 36 Million . . .	Felipe Solferini,Vangelis . . .
11:30 - 12:30	Thin Client? Thin Crypto - Bypassing Full-Disk Enc . . .	Darren McDonald
11:00 - 11:59	Very Pwned: Hacking Verifone's card machine thre . . .	Reino Mostert
11:30 - 12:30	Your OTP Never Arrived: Attacking the Trust Bounda . . .	Kyprianos "kavasilo" Vasi . . .
11:00 - 11:59	Forgotten but Not Gone: Unauthenticated RCEs and L . . .	Ron Ben Yizhak
12:00 - 12:59	Rage Against the Sandbox: Bypassing Apple's iOS . . .	Yuval Hanoach Hirschenbein . . .
12:30 - 13:30	Writing to Shadow Stacks	Vladimir "G1ND1L4" Tokare . . .
12:00 - 12:59	C(2)YA: Inside the Adversary's Inbox	Vitaly Simonovich
12:30 - 13:30	Compounding Interest: Exploiting the ATM Supply Ch . . .	Matt Burch
12:00 - 12:59	The Glass Perimeter: Systematic Bypasses in Biomet . . .	Dan Borgogno,Javier Berna . . .
13:00 - 13:59	gpwn: Wiretapping fiber (GPON) ISP deployments fro . . .	Rithwik "thel3l" Jayasimh . . .
13:30 - 14:30	Bring Your Own Root Of Trust	Mickey "@HackingThings" S . . .
13:00 - 13:59	Stalking the Wily Hacker ... 40 years later	Cliff Stoll
13:30 - 14:30	Transformers: Dark Side of the Type - Weaponizing . . .	Oleksandr Mirosh
13:00 - 13:59	Dylib Hijacking on macOS: Dead or Alive?	Patrick Wardle
14:00 - 14:59	Lights Out: Out-of-Band, Out of Mind, Out of Contr . . .	HD "hdm" Moore
14:30 - 15:30	Bird Hunting Season: The Final Flight	Jon "GainSec" Gaines
14:00 - 14:59	Cracking North Korea's Information Control: How Sm . . .	JDT
14:30 - 15:30	Looking and Peering: Attacking from beyond BGP Adj . . .	Bo-Shiun "bronson113" Yen
14:00 - 14:59	The Enclave is Lying to You: Breaking TEE Trust Bo . . .	Sandeep "pyro" Jayashanka . . .
15:00 - 15:59	Throw Out the Alphabet: Token-Based Markov Chains . . .	Jon "flakpaket" Gorenflo
15:30 - 16:30	Zero-Day Provisioning: Chaining TP-Link ZTP Vulner . . .	Francesco La Spina,Stanis . . .
15:00 - 15:59	Smile, you're on camera! Livestreaming from North . . .	Heiner García,Mauro Eldr . . .
15:30 - 16:30	Wrestling with a Python: Escaping Copilot Studio's . . .	Ryan Hausknecht,Simon Max . . .

PDT Times	Title	speaker
15:00 - 15:59	Get Set, Exploit! Unveiling Python Class Pollution . . .	Gavin Zhong,Zhengyu Liu,J . . .
16:00 - 16:59	Hacking Your Life with AI Can Get You Hacked: How . . .	Peyton "p80n-sec" Kennedy
16:30 - 17:30	How much of our Bluetooth firmware reverse enginee . . .	Veronica Kovah,Xeno Kovah
16:00 - 16:59	The Compiler That Can't Read: Crashing Every 5G Ph . . .	Qiqing Huang,Xingyu Wang
16:30 - 17:30	Taming the Swarm: Hard Architectural Lessons from . . .	Albert "yz9yt" Corzo
16:00 - 16:59	Install Me Maybe: Turning Claimable VS Code Extens . . .	Raphael "rcss" Silva
17:00 - 17:59	High Voltage Heist: Turning Your EV into my Power . . .	Fabien Guillebot,Stepan K . . .
17:30 - 17:59	TEE.fail: Breaking Trusted Execution Environments . . .	Daniel Genkin,Jalen Chuan . . .
17:00 - 17:59	OffGuard: Breaking the Most Popular AI Gateway fro . . .	Yaara Shriki
17:30 - 20:30	DEF CON Franklin: What worked, what didn't, and . . .	Jake Braun
17:00 - 17:59	CRLF-Powered Desync Attacks: Beheading HTTP stream . . .	Tom "t0xodile" Stacey,Tob . . .
Sunday		
10:00 - 10:59	ESP32 as a counter-surveillance platform	Cooper "Cybertiger" Quint . . .
10:00 - 10:59	This Message Was Sent by Microsoft: Turning Micros . . .	Keanu "RedByte" Nys
10:00 - 10:59	Shepherding the Tor network	Roger "arma" Dingleline
10:30 - 11:30	Reversing a Recall: From 'Noise Triggered' to . . .	Ben Gardiner
10:00 - 10:30	Going the Distance: Long-Range Keystroke Injection . . .	Benito "paperclipsvinny" . . .
10:00 - 10:30	No Prompt Required: Pre-Task RCE in Google Gemini . . .	Elad Meged
10:30 - 11:30	Gotta Phish 'Em All! Novel Attack Techniques via P . . .	Giacomo "GiaccoLenzo2109" . . .
11:00 - 11:59	LaunchBreak: a Sip of Tea, a Click, and a Full Mul . . .	Gavin Zhong,Zhengyu Liu,J . . .
11:00 - 11:59	Beyond the Ceremony: The 2026 Passkey Attack Surfa . . .	Matteo Giordano
11:00 - 11:59	Gone in 60 Frames – USB Video Exploitation	Alex Plaskett,Robert Herr . . .
11:30 - 12:30	BLE Theft Auto: How a Dealer-Installed Anti-Theft . . .	Aaron Schulman,Jerry Yu,Y . . .
11:30 - 12:30	From Fuzzer Noise to a Weaponized PHP Exploit: Exp . . .	Can Oztas,Kağan Çapar
12:00 - 12:59	Your WAF Blocked Us, That Was The Exploit - Remote . . .	Barak Sternberg,Nevo Pora . . .
12:00 - 12:59	MSIX'd Up: Weaponizing the Modern Windows App Pack . . .	Nick "zyn3rgy" Powers
12:00 - 12:59	1.1 Million Cameras, One Wildcard: Architectural S . . .	Sammy Azdoufal
12:30 - 13:30	Chaining Microsoft Binaries to get Privileged Prim . . .	Angelo Frasca Caccia
12:30 - 13:30	CUDA've done better - Hacking Nvidia GPUs for cont . . .	Daniel "0xDACA" Cohen Hil . . .
13:30 - 14:59	Contest Closing Ceremonies & Awards	
13:00 - 13:59	Chaining Logical Bugs for Reliable Windows LPE	Bocheng "Crispr" Xiang,He . . .
13:30 - 14:30	Witchcraft Solver: Automated 0day Discovery in Str . . .	Jonathan "endrazine" Bros . . .
13:30 - 13:59	Taking on the Dark Fleet... in Cyberspace!	Kenneth Miltenberger,Shan . . .
14:00 - 14:30	Hacking Jetskis - from Sea-Don't to Sea-Doo	stacksmashing
14:00 - 14:30	Talkers Without Borders: Worldwide Free Speech wit . . .	T. Gwyddon "data" Owen,am . . .
15:00 - 17:30	DEF CON Closing Ceremonies & Awards	Jeff "The Dark Tangent" M . . .

[Return to Index](#)

DEF CON Training

Home Page: <https://training.defcon.org/collections/def-con-training-las-vegas-2026>

PDT Times	Title	speaker
Friday		
08:30 - 17:30	Beat the Breach: Defend, Respond, Survive	McKay Hardy,Wes Wagstaff
08:30 - 17:30	Cyber & AI Policy Basics: What Every Organization ...	Pamela 'Pam' Feld,Greg Go ...
08:30 - 17:30	Digital Supply Chain Security: Software, Cryptogra ...	Anant Shrivastava,Sunil Y ...
Saturday		
08:30 - 17:30	Blue vs Red Bootcamp: From Attacker Playbooks to D ...	Carlo Anez Mazurco,Marian ...
08:30 - 17:30	Influence Operations: Tactics, Defense, and Exploi ...	Greg Conti,Tom Cross
08:30 - 17:30	Full-Stack Pentesting Laboratory: 100% Hands-On + ...	Dawid Czagan
Sunday		
08:30 - 17:30	Blue vs Red Bootcamp: From Attacker Playbooks to D ...	Carlo Anez Mazurco,Marian ...
08:30 - 17:30	Influence Operations: Tactics, Defense, and Exploi ...	Greg Conti,Tom Cross
08:30 - 17:30	Full-Stack Pentesting Laboratory: 100% Hands-On + ...	Dawid Czagan
Monday		
08:30 - 17:30	AI + SOC 101 Bootcamp: Building Modern Security Op ...	Rod Soto
08:30 - 17:30	Dark Wolf Hack Our Drone Workshop	Ronald Broberg,Rudy Mendo ...
08:30 - 17:30	VS: S-RAD (Satellite-Radio Analysis & Disruption)	Andrzej Olchawa,Ricardo F ...
08:30 - 17:30	Agentic AppSec: Harnessing LLMs	Seth Law,Ken Johnson
08:30 - 17:30	Simulated Adversary: Tactics & Tools Training	Jayson E. Street,Iain Jac ...
08:30 - 17:30	Breaking the Cloud Layer - Modern and Practical At ...	Anant Shrivastava,Riyaz W ...
08:30 - 17:30	Securing the Future: Defending Kubernetes & Cloud- ...	Madhu Akula
08:30 - 17:30	Breaking Physical Access Control: Electrical Funda ...	Red Team Alliance
08:30 - 17:30	Advanced Windows Binary Exploitation	Kolja Grassmann,Florian S ...
08:30 - 16:59	Offensive Cyber Security Operations: Mastering Bre ...	Abhijith "Abx" B R
08:30 - 17:30	Analyze, Detect & Hunt: Hands-On Malware Analysis, ...	Monnappa K A,Sajan Shetty
08:30 - 17:30	Blue vs Red Bootcamp: From Attacker Playbooks to D ...	Carlo Anez Mazurco,Marian ...
08:30 - 17:30	Deep Dive into the Dark Web	Robert "pwcraack" Weiss
08:30 - 17:30	Car Hacking Masterclass - Attacking & Defending Au ...	Kamel Ghali
08:30 - 17:30	Adversarial Thinking: The Art of Dangerous Ideas	Greg Conti,Tom Cross
08:30 - 17:30	Black Belt Pentesting / Bug Hunting Millionaire: M ...	Dawid Czagan
08:30 - 17:30	Solving Modern Cybersecurity Problems with AI	Michael Glass
08:30 - 17:30	AI SecureOps: Attacking & Defending AI Application ...	Abhinav Singh
08:30 - 17:30	Agentic RE: Automating Reverse Engineering & Vulne ...	John "clearbluejar" McInt ...
08:30 - 17:30	Advanced Cloud Incident Response in Azure and Micr ...	Korstiaan Stam
08:30 - 17:30	Applied SDR Hacking: Red Team SIGINT for mission-c ...	Jos Wetzels,Wouter Boksla ...
08:30 - 17:30	AI Agent Security Masterclass: Attacking and Defen ...	Abhay Bhargav,Vishnu Pras ...
08:30 - 17:30	Strategic AI Penetration: Mastering Offensive Tech ...	Marek Zmysłowski,Konrad ...
08:30 - 17:30	Bridging the GAP: Hands-On Embedded Hardware Hacki ...	Aaron Wasserman,Garrett F ...

PDT Times	Title	speaker
08:30 - 17:30	Software Defined Radios 101 - Introduction to RF H . . .	Richard Shmel
08:30 - 17:30	Hacking Cryptography	Ruben Gonzalez,Aaron Kais . . .
08:30 - 17:30	IoT Exploitation Masterclass: Hardware & RF Hackin . . .	Smriti Gaba,Yianna Paris
08:30 - 17:30	Hacking Android and IOT Apps by Example	Abraham Aranguren,Abhishe . . .
Tuesday		
08:30 - 17:30	Dark Wolf Hack Our Drone Workshop	Ronald Broberg,Rudy Mendo . . .
08:30 - 17:30	AI + SOC 101 Bootcamp: Building Modern Security Op . . .	Rod Soto
08:30 - 17:30	VS: S-RAD (Satellite-Radio Analysis & Disruption)	Andrzej Olchawa,Ricardo F . . .
08:30 - 17:30	Agentic AppSec: Harnessing LLMs	Seth Law,Ken Johnson
08:30 - 17:30	Simulated Adversary: Tactics & Tools Training	Jayson E. Street,Iain Jac . . .
08:30 - 17:30	Breaking the Cloud Layer - Modern and Practical At . . .	Anant Shrivastava,Riyaz W . . .
08:30 - 17:30	Securing the Future: Defending Kubernetes & Cloud- . . .	Madhu Akula
08:30 - 17:30	Breaking Physical Access Control: Electrical Funda . . .	Red Team Alliance
08:30 - 17:30	Advanced Windows Binary Exploitation	Kolja Grassmann,Florian S . . .
08:30 - 16:59	Offensive Cyber Security Operations: Mastering Bre . . .	Abhijith "Abx" B R
08:30 - 17:30	Analyze, Detect & Hunt: Hands-On Malware Analysis, . . .	Monnappa K A,Sajan Shetty
08:30 - 17:30	Blue vs Red Bootcamp: From Attacker Playbooks to D . . .	Carlo Anez Mazurco,Marian . . .
08:30 - 17:30	Deep Dive into the Dark Web	Robert "pwcrcrack" Weiss
08:30 - 17:30	Car Hacking Masterclass - Attacking & Defending Au . . .	Kamel Ghali
08:30 - 17:30	Adversarial Thinking: The Art of Dangerous Ideas	Greg Conti,Tom Cross
08:30 - 17:30	Black Belt Pentesting / Bug Hunting Millionaire: M . . .	Dawid Czagan
08:30 - 17:30	Solving Modern Cybersecurity Problems with AI	Michael Glass
08:30 - 17:30	AI SecureOps: Attacking & Defending AI Application . . .	Abhinav Singh
08:30 - 17:30	Agentic RE: Automating Reverse Engineering & Vulne . . .	John "clearbluejar" McInt . . .
08:30 - 17:30	Advanced Cloud Incident Response in Azure and Micr . . .	Korstiaan Stam
08:30 - 17:30	Applied SDR Hacking: Red Team SIGINT for mission-c . . .	Jos Wetzels,Wouter Boksla . . .
08:30 - 17:30	AI Agent Security Masterclass: Attacking and Defen . . .	Abhay Bhargav,Vishnu Pras . . .
08:30 - 17:30	Strategic AI Penetration: Mastering Offensive Tech . . .	Marek Zmysłowski,Konrad . . .
08:30 - 17:30	Bridging the GAP: Hands-On Embedded Hardware Hacki . . .	Aaron Wasserman,Garrett F . . .
08:30 - 17:30	Software Defined Radios 101 - Introduction to RF H . . .	Richard Shmel
08:30 - 17:30	Hacking Cryptography	Ruben Gonzalez,Aaron Kais . . .
08:30 - 17:30	IoT Exploitation Masterclass: Hardware & RF Hackin . . .	Smriti Gaba,Yianna Paris
08:30 - 17:30	Hacking Android and IOT Apps by Example	Abraham Aranguren,Abhishe . . .

[Return to Index](#)

DEF CON Workshops

Home Page: <https://defcon.outel.org/dcwp/dc34/activities/workshops/>

PDT Times	Title	speaker
Friday		
09:00 - 12:59	Sold Out - Offensive Packet Wizardry with Scapy	Mike "Chicolinux" Guirao
09:00 - 12:59	Sold Out - Hands-on IoT firmware extraction and fl...	Dennis Giese,Braelynn Lue...
09:00 - 12:59	Sold Out - AWS Cloud Security 101: From IAM Miscon...	zeta,Rafa "bane" Gutierre...
09:00 - 12:59	Sold Out - Web Hacking 101	cale "calebot" smith,Ruch...
09:00 - 12:59	Sold Out - Malware Development 101 - From Zero to ...	Yoann "OtterHacker" DEQUE...
09:00 - 12:59	Sold Out - Long Live Empire: A C2 Workshop for Mod ...	Jake "Hubbl3" Krasnov,Vin...
09:00 - 12:59	Sold Out - Learning to Hack Bluetooth Low Energy w ...	Ryan "Hackgnar" Holeman,A...
09:00 - 12:59	Sold Out - Agentic Threat Hunting: Building AI Tha ...	Sydney "letswastetime" Ma...
14:00 - 17:59	Sold Out - Investigating and Responding to M365 ac ...	Vince "bitpusher" Weppner
14:00 - 17:59	Sold Out - OT Systems: how to secure them in pract ...	Alexandrine Torrents,Arna...
14:00 - 17:59	Sold Out - AWS Principal Threat Hunting: Behaviora ...	Rodrigo "Sp0oKeR" Montoro
14:00 - 17:59	Sold Out - Reaching Mythos: Hands-On Vulnerability ...	John "clearbluejar" McInt...
14:00 - 17:59	Sold Out - Solder, Detect, Listen: Build Your Own ...	Darcy "@Drc3p0" Neal
14:00 - 17:59	Sold Out - All About Stoopie InfoStealers: Malware ...	Ryan "@rj_chap" Chapman,A...
14:00 - 17:59	Sold Out - Introduction to Malware Analysis	Sam Bowne,Elizabeth Biddl...
14:00 - 17:59	Sold Out - Embedded Computing Tools for Wireless H ...	Joseph Long
Saturday		
09:00 - 12:59	Sold Out - Wi-Fight Club: I am Jack's Evil Twin	James Hawk,Jon "C4V3M4N"...
09:00 - 12:59	Sold Out - Explore the Windows instrumentation cal ...	Yoann "OtterHacker" DEQUE...
09:00 - 12:59	Sold Out - Step-by-Step Malware Development: Evadi ...	Yu Terada,Kotaro "@Decama...
09:00 - 12:59	Sold Out - Words As Weapons: Breaking AI and Agent ...	Pavan "pavanreddysec" Red...
09:00 - 12:59	Sold Out - HackTheCloud26: Chaining Cloud Misconfi ...	HackeMate
09:00 - 12:59	Sold Out - Hecate: A Trivial UART Tool	mx,Joe "SecurelyFitz" Fit...
09:00 - 12:59	Sold Out - Detecting and Analyzing Memory Only Mal ...	Andrew Case,Pierre "Abyss...
09:00 - 12:59	Sold Out - Battle-Tested Broadcasts: RF Insights F ...	Preston Zen
14:00 - 17:59	Sold Out - Hands-on DuckyScript: An Introduction t ...	wasabi,Ø1,Tokugero
14:00 - 17:59	Sold Out - Purple Teaming Industrial Control Syste ...	Arnaud SOULLIE,Alexandrin...
14:00 - 17:59	Sold Out - Entra ID Persistence - Because Password ...	Raunak "Trouble1" Parmar,...
14:00 - 17:59	Sold Out - From Prompt to PWN: Exploiting LLM Powe ...	Abhinav Verma
14:00 - 17:59	Sold Out - Intro to Writing Windows Malware with R ...	iDigitalFlame,Daniel Brav...
14:00 - 17:59	Sold Out - Building Agentic Reverse Engineering "S ...	John "clearbluejar" McInt...
14:00 - 17:59	Sold Out - Learning to Reverse Engineer Compiled C ...	Wesley McGrew
14:00 - 17:59	Sold Out - Salesforce Apex Predator: Breaking Sale ...	Nitay Bachrach,Cynthia Ar...
Sunday		
09:00 - 12:59	Sold Out - Attacking Cloud APIs from the IoT Edge	Rodney "BenevolentWorm" B...
09:00 - 12:59	Sold Out - Building your own hardware hacking kit ...	Dallas

PDT Times	Title	speaker
09:00 - 12:59	Sold Out - Post-Quantum Cryptography (PQC) for Hac . . .	Eric "Eijah" Anderson
09:00 - 12:59	Sold Out - Purple Protocol: Adversary emulation fo . . .	Patrick "PilotPat" Raiden . . .
09:00 - 12:59	Sold Out - CI/CD Weaponization: Build It, Deploy I . . .	Ricardo Sanchez,Daniel Ma . . .
09:00 - 12:59	Sold Out - ICS Hack 'n Track	Pedro Cabrera,Hannes "her . . .
09:00 - 12:59	Sold Out - Creating Shellcode for Hackers	Bramwell "Bw3ll" Brizendi . . .
09:00 - 12:59	Sold Out - Pivot, Hunt, Publish: An Offline, Hands . . .	Rushikesh Nandedkar

[Return to Index](#)

Demo Labs

Home Page: <https://defcon.outel.org/dcwp/dc34/activities/dl/>

PDT Times	Title	speaker
Friday		
10:00 - 10:45	AD-Necromancer: Resurrecting Forgotten Control Pat . . .	Akbar "0xsensei" Abdullay . . .
10:00 - 10:45	Peekaboo: Breaking the Black Box of Threat and Mal . . .	Zhassulan "cocomelonc" Zh . . .
10:00 - 10:45	Senrigan () x Suzaku (): Threat Hun . . .	Fukusuke Takahashi,Zach M . . .
10:00 - 10:45	X-Ray Your Agents: Pentesting MCPs, Skills, and th . . .	Xia Hua,Abhijeet Kumar
10:00 - 10:45	PromptPwn: Finding and Exploiting AI-Generated Vul . . .	Georgia Weidman
10:00 - 10:45	Empire 7: Shipping a C2 at AI Speed	Vincent "Vinnybod" Rose,J . . .
11:00 - 11:45	Damn Vulnerable Agentic AI Application (DVAIA)	Abhinav Verma,Mukesh Agga . . .
11:00 - 11:45	sisakulint:CI-Friendly static linter with autofix, . . .	Atsushi Sada,hikae
11:00 - 11:45	Be like a BRAT(BLE Recon and Attack Toolkit): Skip . . .	Gigi Xiaoqing Liu,Muzzamm . . .
11:00 - 11:45	Zealot: An Autonomous Cloud Offensive Multi-Agent . . .	Chen Doytshman
11:00 - 11:45	AOBTD: AI One Bites The DAST	Ozgun "ozzy" Kultekin
11:00 - 11:45	AI Pipeline for N-days Weaponization	Andrea Brosio,Arun Nair
12:00 - 12:45	Damn Vulnerable Agentic AI Application (DVAIA)	Abhinav Verma,Mukesh Agga . . .
12:00 - 12:45	GnawLab: Open-Source AWS Attack Scenarios Based on . . .	ialleejy,Kyul,HyunJun "Be . . .
12:00 - 12:45	VoiceLock: Offline, Robust On-Device Speech Transc . . .	Ayaan Qayyum,Parag Kalay
12:00 - 12:45	Ghost in the IDE	Venkata Jayaram Yalla,Par . . .
12:00 - 12:45	Weaponizing eBPF and XDP with Covert Triggered Rev . . .	Yll "0xBabar0ka" Berisha
12:00 - 12:45	Overcast: Video OSINT Agent. Point It at 100 Video . . .	Kevin "kdrwins" Dela Rosa
13:00 - 13:45	xEndity: IoT Firmware Analysis & Digital Twin Plat . . .	Zeus "LightningGod" Chan, . . .
13:00 - 13:45	MSCodePhish: Redeem Your Coupon. Surrender Your Se . . .	Raunak "Trouble1" Parmar, . . .
13:00 - 13:45	Goose Processing Unit (GPU): VRAM as an Unmonitore . . .	Gannon "Dorf" Gebauer,Ant . . .
13:00 - 13:45	Zero-Cloud Threat Modeling: Vector Embedding Archi . . .	Ankit Vashisth
13:00 - 13:45	Beyond Spidering: Behavior Driven DAST for Real Ap . . .	Sara "testingSoul" Martin . . .
13:00 - 13:45	Monitor, Compile, Enforce: A Compiler Pipeline for . . .	Buğrahan Yücel
14:00 - 14:45	SecretSifter: Production Apps Are Leaking Credenti . . .	Hemanth Gorijala
14:00 - 14:45	MalSkill Lab: Hands-On Natural Language Malware in . . .	Nur "BurritoTheNurrito" G . . .
14:00 - 14:45	Clew: Untangling Evasive Malware with Per-Sample F . . .	Kyler McElroy,Anita Ding, . . .
14:00 - 14:45	AzProwl: Prowling the Azure Attack Surface	Jared "GonePhishing402" G . . .
14:00 - 14:45	L.A.Y.E.R.S - Layered Analysis Engine for Browser . . .	Abhinav Khanna,Krishna Ch . . .
14:00 - 14:45	Trajan: Cross-Platform CI/CD Security Scanner	Rahul Saranjame,Ranganath . . .
15:00 - 15:45	GhostCatcher (endpoint detection agent)	Sercan Okur
15:00 - 15:45	Intercept.js: Runtime-Aware Detection for JavaScri . . .	Rishi Kant
15:00 - 15:45	BigIron.ai: AI-Assisted Exploration and Security A . . .	Adam "w00tock" Toscher
15:00 - 15:45	AzProwl: Prowling the Azure Attack Surface	Jared "GonePhishing402" G . . .
15:00 - 15:45	TokenMesh: Exposing Azure's Hidden Identity Attack . . .	Saksham Agrawal
15:00 - 15:45	pymSI: Interactive MSI Installer Analysis in Pytho . . .	Ryan "Nightlark" Mast
16:00 - 16:45	Phasmid: Deniable Storage for Rubber-Hose Scenario . . .	Makoto "Mr.Rabbit" Sugita

PDT Times	Title	speaker
16:00 - 16:45	AC Scanner: The Post-Quantum Cryptographic Exposur . . .	Anurag Swarnim Yadav,Jose . . .
16:00 - 16:45	BigIron.ai: AI-Assisted Exploration and Security A . . .	Adam "w00tock" Toscher
16:00 - 16:45	DFMI: Weaponizing MSI Installers for Fileless Code . . .	Anil Celik
16:00 - 16:45	Reversing F5: Pure-Go Steganography, Live Forensic . . .	Overkilll
16:00 - 16:45	MailX-Ray: A TSA X-Ray for Emails — Air-Gapped S . . .	Uğur "uJohn" Can ATASOY
Saturday		
10:00 - 10:45	SecretSifter: Production Apps Are Leaking Credenti . . .	Hemanth Gorijala
10:00 - 10:45	Peekaboo: Breaking the Black Box of Threat and Mal . . .	Zhassulan "cocomelonc" Zh . . .
10:00 - 10:45	Goose Processing Unit (GPU): VRAM as an Unmonitore . . .	Gannon "Dorf" Gebauer,Ant . . .
10:00 - 10:45	DFMI: Weaponizing MSI Installers for Fileless Code . . .	Anil Celik
10:00 - 10:45	Reversing F5: Pure-Go Steganography, Live Forensic . . .	Overkilll
10:00 - 10:45	Monitor, Compile, Enforce: A Compiler Pipeline for . . .	Buğrahan Yücel
11:00 - 11:45	GhostCatcher (endpoint detection agent)	Sercan Okur
11:00 - 11:45	sisakulint:CI-Friendly static linter with autofix, . . .	Atsushi Sada,hikae
11:00 - 11:45	Clew: Untangling Evasive Malware with Per-Sample F . . .	Kyler McElroy,Anita Ding, . . .
11:00 - 11:45	X-Ray Your Agents: Pentesting MCPs, Skills, and th . . .	Xia Hua,Abhijeet Kumar
11:00 - 11:45	TokenMesh: Exposing Azure's Hidden Identity Attack . . .	Saksham Agrawal
11:00 - 11:45	pymSI: Interactive MSI Installer Analysis in Pytho . . .	Ryan "Nightlark" Mast
12:00 - 12:45	Phasmid: Deniable Storage for Rubber-Hose Scenario . . .	Makoto "Mr.Rabbit" Sugita
12:00 - 12:45	MSCodePhish: Redeem Your Coupon. Surrender Your Se . . .	Raunak "Trouble1" Parmar, . . .
12:00 - 12:45	Keychecker : SSH Key based attack tool for DVCS Sy . . .	Anant Shrivastava
12:00 - 12:45	Zealot: An Autonomous Cloud Offensive Multi-Agent . . .	Chen Doytshman
12:00 - 12:45	Beyond Spidering: Behavior Driven DAST for Real Ap . . .	Sara "testingSoul" Martin . . .
12:00 - 12:45	Empire 7: Shipping a C2 at AI Speed	Vincent "Vinnybod" Rose,J . . .
13:00 - 13:45	AD-Necromancer: Resurrecting Forgotten Control Pat . . .	Akbar "0xsensei" Abdullay . . .
13:00 - 13:45	MalSkill Lab: Hands-On Natural Language Malware in . . .	Nur "BurritoTheNurrito" G . . .
13:00 - 13:45	Keychecker : SSH Key based attack tool for DVCS Sy . . .	Anant Shrivastava
13:00 - 13:45	Hook Crook - Extracting More From Discord Webhooks	Jeremy Banker - K0JLB,Ari . . .
13:00 - 13:45	L.A.Y.E.R.S - Layered Analysis Engine for Browser . . .	Abhinav Khanna,Krishna Ch . . .
13:00 - 13:45	Trajan: Cross-Platform CI/CD Security Scanner	Rahul Saranjame,Ranganath . . .
14:00 - 14:45	LoKi: A LoRa/Meshtastic based implant for Red Team . . .	Venky Raju
14:00 - 14:45	Intercept.js: Runtime-Aware Detection for JavaScri . . .	Rishi Kant
14:00 - 14:45	Senrigan () x Suzaku (): Threat Hun . . .	Fukusuke Takahashi,Zach M . . .
14:00 - 14:45	Hook Crook - Extracting More From Discord Webhooks	Jeremy Banker - K0JLB,Ari . . .
14:00 - 14:45	PromptPwn: Finding and Exploiting AI-Generated Vul . . .	Georgia Weidman
14:00 - 14:45	MailX-Ray: A TSA X-Ray for Emails — Air-Gapped S . . .	Uğur "uJohn" Can ATASOY
15:00 - 15:45	LoKi: A LoRa/Meshtastic based implant for Red Team . . .	Venky Raju
15:00 - 15:45	AC Scanner: The Post-Quantum Cryptographic Exposur . . .	Anurag Swarnim Yadav,Jose . . .
15:00 - 15:45	Be like a BRAT(BLE Recon and Attack Toolkit): Skip . . .	Gigi Xiaoqing Liu,Muzzamm . . .
15:00 - 15:45	Ghost in the IDE	Venkata Jayaram Yalla,Par . . .
15:00 - 15:45	AOBTD: AI One Bites The DAST	Ozgun "ozzy" Kultekin
15:00 - 15:45	AI Pipeline for N-days Weaponization	Andrea Brosio,Arun Nair
16:00 - 16:45	xEndity: IoT Firmware Analysis & Digital Twin Plat . . .	Zeus "LightningGod" Chan, . . .

PDT Times	Title	speaker
16:00 - 16:45	GnawLab: Open-Source AWS Attack Scenarios Based on ...	ialleejy,Kyul,HyunJun "Be ...
16:00 - 16:45	VoiceLock: Offline, Robust On-Device Speech Transc ...	Ayaan Qayyum,Parag Kalay
16:00 - 16:45	Zero-Cloud Threat Modeling: Vector Embedding Archi ...	Ankit Vashisth
16:00 - 16:45	Weaponizing eBPF and XDP with Covert Triggered Rev ...	Yll "0xBabar0ka" Berisha
16:00 - 16:45	Overcast: Video OSINT Agent. Point It at 100 Video ...	Kevin "kdrwins" Dela Rosa

[Return to Index](#)

Embedded Systems Village

Location: LVCCW Level 1 Hall 2 503 (Embedded Systems Village) - [Map](#)

Home Page: <https://embeddedvillage.org/>

PDT Times	Title	speaker
Friday		
10:00 - 17:59	Embedded - 101 Labs	
10:00 - 17:59	Exploit Bluetooth Low Energy with BLESPlloit and op . . .	Slawomir Jasek
10:00 - 17:59	Embedded Systems Village CTF	
Saturday		
10:00 - 17:59	Exploit Bluetooth Low Energy with BLESPlloit and op . . .	Slawomir Jasek
10:00 - 17:59	Embedded Systems Village CTF	
10:00 - 17:59	Embedded - 101 Labs	
10:00 - 17:59	Thread Carefully	
Sunday		
10:00 - 13:59	Embedded - 101 Labs	
10:00 - 13:59	Embedded Systems Village CTF	
10:00 - 13:59	Exploit Bluetooth Low Energy with BLESPlloit and op . . .	Slawomir Jasek

[Return to Index](#)

Game Hacking Village

Location: LVCCW Level 1 Hall 1 211 (Game Hacking Village) - [Map](#)

Home Page: <https://gamehacking.gg/>

PDT Times	Title	speaker
Friday		
10:00 - 15:59	Chill Zone: Casual Games & TASBot Smash Demo	
12:00 - 16:59	Riot Games Vanguard: Pwn to own	
14:00 - 14:59	iOS Game Hacking : From Zero to GOD Mode	M41w4r3
14:45 - 15:45	Your Lives are in Another Struct: Breaking Memory . . .	Ryan Zmuda
16:00 - 16:59	Bobba! A Complete History of Habbo Hotel Private S . . .	InsiderPHD
16:00 - 16:59	Chill Zone: Smash (Project Plus) Tournament with P . . .	
Saturday		
10:00 - 16:59	Riot Games Vanguard: Pwn to own	
10:00 - 15:59	Chill Zone: Casual Games & TASBot Smash Demo	
10:00 - 10:45	RIP Denuvo: DRM in a Post-Hypervisor World	Amin Hussien
10:45 - 11:30	Dreamcast Ex Inferis: RCE on the Sega Dreamcast Pl . . .	Christopher Hernandez
11:30 - 11:59	Catching Cheaters in Super Smash Bros Melee	AltF4
12:00 - 12:59	Game Hacking with AI	Juno
14:00 - 14:59	Catching Cheaters in Super Smash Bros Melee	AltF4
16:00 - 16:59	Chill Zone: Smash (Project Plus) Tournament with P . . .	
16:00 - 16:59	Dreamcast Ex Inferis — RCE on the Sega Dreamcast . . .	Piffd0s
Sunday		
11:30 - 12:30	Yes, I froze an SNES for science	dwangoAC
12:30 - 12:59	SH4ZAM: Accelerated Vector Math on the Sega Dreamc . . .	Falco Girgis

[Return to Index](#)

Hackers.town

Home Page: <https://masto.hackers.town/>

PDT Times	Title	speaker
Friday		
11:00 - 11:30	Tech Reclaimers Update: A Year In, Building a Soci . . .	Andy Hull,Janet Vertesi,R . . .
11:00 - 11:59	building community and privacy tools from junk	TheGibson
13:00 - 13:30	The Cum-Stained Precipice of Digital Redlining	Erica Rachel Andrews,Abbi . . .
13:00 - 13:59	Liberate your Music with Tech Reclaimers	RemoteNemesis
14:00 - 14:59	Too Much "Slop" and Not Enough Soul: Why the AI Mu . . .	RabidMoosery
15:00 - 15:59	The Political economy of AI	Janet Vertesi
16:00 - 16:59	Hackers Trivia	RemoteNemesis,Medus4
Saturday		
11:00 - 11:59	How to get RCE on a car	Ac0rn
12:00 - 12:30	KYC and XMR... FOR HACKERS!	AltKey
12:00 - 12:59	Take Back Your Memories	Patrick Sliney
14:00 - 14:59	Fun with alternative smartphones with The Tech Rec . . .	Janet Vertesi
15:00 - 15:59	The Enshittified Internet and How We Can All Rewil . . .	LambdaCalculus
Sunday		
10:30 - 10:59	The Enshittified Internet and How We Can All Rewil . . .	LambdaCalculus

[Return to Index](#)

Ham Radio Village

Location: LVCCW Level 3 W315 (Ham Radio Village) - [Map](#)

Home Page: <https://hamvillage.org/>

Sched Page: <https://cfp.hamvillage.org/dc34/talk/>

PDT Times	Title	speaker
Friday		
11:00 - 11:30	Meshtastic 101: Off-Grid Mesh Networking with LoRa	Jon Marler (K4CHN)
12:00 - 12:30	Getting Started In Radio Direction Finding	Nate Moore
13:00 - 13:59	Ham Radio Isn't Magic: Preppers, Sad Hams, and P . . .	Andrew Ohnstad - N3OCQ
14:30 - 15:10	Who Owns Your Shack? Open Source, Amateur Radio, a . . .	Jeremy Banker - K0JLB
15:30 - 16:18	Advanced Topics in LoRa Meshes	Eric Escobar
Saturday		
11:00 - 11:30	Digital Modes 101: The Weird, Wonderful World of C . . .	Jon Marler (K4CHN)
12:00 - 12:30	So You Got Your License, Now What?	Danny Quist
13:00 - 13:30	Why Signals Still Matter: Amateur Radio in the Age . . .	Nate Moore
14:30 - 14:59	Ham Radio - Licensed to Experiment	Dan W0BDP Norte
15:00 - 15:50	Meshtastic Beasts and Where to Find Them	Scott Thompson
16:00 - 16:45	Keeping the Angry Pixies Happy: the Care and Feedi . . .	hamster
Sunday		
10:00 - 11:30	"Can it Ham" Antenna Testing	The HRV Contest Team

[Return to Index](#)

ICS Village

Location: LVCCW Level 1 Hall 2 502 (ICS Village) - [Map](#)

Home Page: <https://www.icsvillage.com/>

Sched Page: <https://icsvillage.com/defcon-34>

PDT Times	Title	speaker
Friday		
11:00 - 11:59	Intro to Common Industrial Protocol Exploitation	Trevor Flynn
12:00 - 12:30	Threat Hunting in OT Networks - Using Hypothesis B . . .	Michael Cardwell
14:30 - 14:59	ICSForge: (Open-Source) OT/ICS Security Coverage V . . .	Can Kurnaz
15:00 - 15:30	OT Segmentation Under Operational Constraints	Tony Turner
17:00 - 17:30	Lessons Learned from Poland and Beyond: The State . . .	Joe Slowik
17:30 - 17:59	Exposed Data Centers: Bypass IT Security, Crank Up . . .	Stephen Hilt,Numaan Huq
Saturday		
11:30 - 11:59	Nuclear Industrial Control System Simulation (NICS . . .	Carmela Gonzales,Brian G. . . .
12:00 - 12:30	Local Language Models in OT - Basics and Considera . . .	Vivek Ponnada
14:45 - 15:30	Give an AI Industrial Protocol Tools and Watch Wha . . .	Malav Vyas,Asher Davila
14:00 - 14:45	OT Round table. Real talk on how to protect your O . . .	Aaron Crow,Tom VanNorman, . . .
Sunday		
10:00 - 10:30	Five Million Industrial Control Systems Walk Into . . .	Matt Caldwell
11:00 - 11:30	Is Your Fridge Running? Then You Better Catch It - . . .	Amir Zaltzman
12:30 - 12:59	Two NICs, Zero Trust: Pulling Apart a PAC Buried i . . .	Adam Bromiley,Sam Thom
12:00 - 12:30	ThreatPatrol: Visualising the Modern Threat Landsc . . .	Viral Maniar

[Return to Index](#)

IoT Village

Location: LVCCW Level 1 Hall 1 215 (IoT Village) - [Map](#)

Home Page: <https://www.iotvillage.org/>

Sched Page: <https://www.iotvillage.org/events/defcon-34/index.html>

PDT Times	Title	speaker
Friday		
10:00 - 17:59	All About UART	
10:00 - 17:59	Expose Hidden Surveillance in Everyday Tech	
10:00 - 17:59	Hands-On Hardware Hacking – From JTAG to Root, M . . .	
10:00 - 17:59	Just Hacking Training	
10:00 - 17:59	Smart Home in the Matter: Blink, Race, Attack CTF	
10:30 - 11:30	Make your very own evil IoT Cat Lamp with WLED!	Nick
10:00 - 17:59	Raiders of the Lost Firmware: A Hands-On Workshop . . .	
10:00 - 17:59	Cat-apostrophic Hacking: Breaking Into Smart Litter . . .	
10:00 - 17:59	Discover GE Appliances!	
10:45 - 11:30	Sick Signals: Adversarial Prompt Injection via Med . . .	Vinitha Mathiyazhagan,Tam . . .
12:00 - 13:30	Build Your Own Meshtastic Node: Off-Grid, Encrypte . . .	Kody Kinzie
12:30 - 13:15	Dr. Strangepwn: How I Learned to Stop Worrying and . . .	Larry Pesce
13:45 - 15:15	Mesh Nets for Hackers: How (& When) to use Meshtas . . .	Kody Kinzie
15:45 - 17:15	Wi-Fi Self Defense & Hacker Hunting & For Beginner . . .	Kody Kinzie
Saturday		
10:30 - 11:45	Playing with Hyper-local Pocket-Sized Servers	Brandon
10:00 - 17:59	Discover GE Appliances!	
10:00 - 17:59	All About UART	
10:00 - 17:59	Raiders of the Lost Firmware: A Hands-On Workshop . . .	
10:00 - 17:59	Smart Home in the Matter: Blink, Race, Attack CTF	
10:00 - 17:59	Just Hacking Training	
10:00 - 17:59	Hands-On Hardware Hacking – From JTAG to Root, M . . .	
10:00 - 17:59	Expose Hidden Surveillance in Everyday Tech	
10:00 - 17:59	Cat-apostrophic Hacking: Breaking Into Smart Litter . . .	
11:45 - 12:30	Anyone Can Hack IoT (Even Easier Now) - A Beginner . . .	Andrew Bellini
11:00 - 11:45	The Camera Is Lying: RTSP Trust Failures in Modern . . .	Bogdan "BOTEZATU"
12:00 - 13:30	Wi-Fi Self Defense & Hacker Hunting & For Beginner . . .	Kody Kinzie
12:30 - 13:30	Raiders of the Lost Firmware: A Hands-On Workshop . . .	Simone Bossi, Luca Borzacc . . .
14:30 - 15:15	UAiRT: Over The Air UART	Metehan Arslan, Samet Berk . . .
15:00 - 16:30	Mesh Nets for Hackers: How (& When) to use Meshtas . . .	Kody Kinzie
15:15 - 15:59	Beyond Your Bookshelf: Hackable eReaders	Katie Paxton-Fear
16:30 - 17:30	Weaponization of Cellular Based IoT Technology – . . .	Carlota Bindner, Deral Hei . . .
Sunday		
10:00 - 13:59	Just Hacking Training	
10:00 - 13:59	Cat-apostrophic Hacking: Breaking Into Smart Litter . . .	

PDT Times	Title	speaker
10:00 - 13:59	Hands-On Hardware Hacking – From JTAG to Root, M . . .	
10:00 - 13:59	Raiders of the Lost Firmware: A Hands-On Workshop . . .	
10:00 - 13:59	Discover GE Appliances!	
10:00 - 13:59	All About UART	
10:00 - 13:59	Smart Home in the Matter: Blink, Race, Attack CTF	
10:00 - 13:59	Expose Hidden Surveillance in Everyday Tech	
10:15 - 10:59	Make your very own evil IoT Cat Lamp with WLED!	Nick
10:00 - 10:59	You Can't Opt Out: The Invisible Surveillance in Y . . .	Naomi Brockwell
11:00 - 13:30	Wi-Fi Self Defense & Hacker Hunting & For Beginner . . .	Kody Kinzie
11:30 - 11:59	One Firmware Flaw, 70+ Device Models: Lessons in I . . .	Weihan Goh,ZhengChao Wen

[Return to Index](#)

La Villa Community

Home Page: <https://lavillahacker.com/>

PDT Times	Title	speaker
Friday		
10:00 - 10:30	La Villa - Opening Ceremony (ESP)	
10:30 - 11:30	Bootkits Forever: Emulando APTs Modernos desde UEF . . .	Alejandro Vázquez Vázqu . . .
10:30 - 12:59	De la nube a la corona: Uso indebido de la identid . . .	Juan Camilo Palacio Arang . . .
11:30 - 12:30	Demodus Operandi (Cómo tres rf-hacks en tres band . . .	Eduardo Contreras
12:30 - 12:59	O Lado Sombrio das Coisas: Transformando Dispositi . . .	Christiane Borges Santos
13:00 - 13:59	AImaru C2: La Nueva Era del Living off the Land (M . . .	Mario Lobo
14:00 - 14:59	Point of Failure: Autopsia de una Terminal de Pago	Erik Alcantara
14:00 - 15:59	PentestGPT: The Art of Hacking with Words	Matias Armándola
15:00 - 15:30	El regreso de Sedinho: situación actual y nuevas . . .	Josep Albors
15:30 - 15:59	State Desync as a Weapon: Breaking Transactional I . . .	Santiago Sepúlveda Veliz
16:00 - 16:59	Jackpoting? Bypass de EDR? - Hacking ATM	Arnold Jared Morales Yepe . . .
17:00 - 17:59	Tokens and PRT: Advanced Attacks and Persistence i . . .	Elzer Pineda,Jose Rivas
Saturday		
10:00 - 10:30	Learning Deception by Doing: Attacking and Defendi . . .	Diego Staino,Fede Pacheco
10:30 - 10:59	Self Hosting Nightmare - Exploiting AI models for . . .	Davidson Mizael
10:30 - 12:59	Workshop Before the SIEM Blinks: How AI Memory Tur . . .	Luis Pazmino,Yoshihito Ad . . .
11:00 - 11:59	Meet XEntry Team: A powerful threat actor abusing . . .	Eduardo Chavarro Ovalle
12:00 - 12:30	Malware Inc.: Cybercrime-as-a-Service y la econom. . .	Isabel Manjarrez
12:30 - 13:30	Descubrimiento Industrializado de CVEs con Agentes . . .	Simon Correa,Michael Rive . . .
13:30 - 13:59	The CVE-Hunters Project: From Noobs to Researchers	Natan Morette
14:00 - 14:30	Keep the Model on Course: Agentic LLM Workflows fo . . .	Asher Davila,Lenin Alevsk . . .
14:30 - 15:30	When Cash Runs on Windows: A Red Team Look at ATM . . .	Gerardo Mejia
14:00 - 15:59	Execution of modern techniques to start/improve yo . . .	Ashley Hiram Muñoz
15:30 - 16:30	From Live Malware to Red Team Tradecraft: Process . . .	Filipi Pires
16:30 - 17:30	De la Explotación de Buffer Overflows al C2 Indus . . .	Fernando Mengali
17:30 - 18:30	latinas.exe has entered the chat (ESP - POR)	
Sunday		
10:00 - 10:30	Tu foco IoT nunca tuvo modelo de amenazas	Andres Sabas
10:30 - 11:30	Bait the Bot: Hacking Back Autonomous AI Vulnerabi . . .	Alcyon Junior
11:30 - 11:59	La Rosa de Guadalupe DFIR: Serie de 3 capítulos d . . .	Victor Gomez,Horacio Baz. . .
12:00 - 12:59	Red Robin: Don't Hack For Me, Hack With Me	Juan Sequeira Piedra,Jose . . .
13:00 - 13:30	La Villa - Closing Ceremony (ESP)	

[Return to Index](#)

Lockpick Village

PDT Times	Title	speaker
Friday		
10:15 - 10:45	Intro to Lockpicking	
11:00 - 11:59	Building an open soure safecracking robot	Jared Dygert
13:00 - 13:30	Intro to Lockpicking	
14:30 - 14:59	Intro to Lockpicking	
16:00 - 16:30	Intro to Lockpicking	
Saturday		
10:15 - 10:45	Intro to Lockpicking	
11:00 - 11:30	Classic US High Sec: how to pick a Medeco	Max A
15:00 - 15:30	Intro to Lockpicking	
Sunday		
10:15 - 10:45	Intro to Lockpicking	
11:00 - 11:45	The Knox Box - A Brief History(Part II)	Matthew O'Reilly
13:00 - 13:30	Intro to Lockpicking	

[Return to Index](#)

Lonely Hackers Club

Home Page: <https://lonelyhackers.club/>

PDT Times	Title	speaker
Friday		
10:00 - 17:59	Lonely Hackers Club - Lockpicking Table	
10:00 - 17:59	Lonely Hackers Club CTF	
10:30 - 16:30	Resume Review with the Lonely Hackers Club	
10:00 - 17:59	Lonely Hackers Club - Sticker Swap Table	
Saturday		
10:00 - 17:59	Lonely Hackers Club - Sticker Swap Table	
10:00 - 17:59	Lonely Hackers Club - Lockpicking Table	
10:00 - 17:59	Lonely Hackers Club CTF	
10:30 - 16:30	Resume Review with the Lonely Hackers Club	
Sunday		
10:00 - 13:59	Lonely Hackers Club - Sticker Swap Table	
10:00 - 11:59	Lonely Hackers Club CTF	
10:00 - 13:59	Lonely Hackers Club - Lockpicking Table	
12:00 - 12:59	Lonely Hackers Club - CTF Winners Announcement	

[Return to Index](#)

Maker's Village

Location: LVCCW Level 1 Hall 1 301 (Makers' Village) - [Map](#)

Home Page: <https://makersvillage.space/>

Sched Page: <https://makersvillage.space/#content16-23>

PDT Times	Title	speaker
Friday		
10:00 - 17:59	Makers' Village - Hacker Arts and Crafts	
11:00 - 12:30	Build-A-Badge Workshop	hunny,Teazee,Buddha,MLP,M . . .
12:00 - 12:59	Hardhat How-to	m0nkeydrag0n,MrBill
14:00 - 15:30	Build-A-Badge Workshop	hunny,Teazee,Buddha,MLP,M . . .
15:00 - 16:59	Cyberdeck Build	Sk!tz0
Saturday		
10:00 - 17:59	Makers' Village - Hacker Arts and Crafts	
11:00 - 12:30	Build-A-Badge Workshop	hunny,Teazee,Buddha,MLP,M . . .
13:00 - 13:59	Crafting the Future: DEF CON 34 Light-Up Bow Works . . .	
14:15 - 14:45	Operation Restoration	Cannibal
15:00 - 16:59	Cyberdeck Build	Sk!tz0
16:00 - 17:45	Building Silkscreens and carving stamps	hunny
Sunday		
10:00 - 13:59	Makers' Village - Hacker Arts and Crafts	
11:00 - 11:59	3d Designing basics, 5 minute prints in Tinkercad	hunny
12:00 - 12:59	Novice design in 3d space	RedThorn
13:30 - 13:59	Visable Mending, repair and reinforce	

[Return to Index](#)

Malware Village

Location: LVCCW Level 1 Hall 2 600 (Malware Village) - [Map](#)

Home Page: <https://malwarevillage.org/>

PDT Times	Title	speaker
Friday		
10:55 - 11:35	Lyra: An LLVM IR Obfuscator for Rust	Rafael Felix
10:00 - 10:45	Anatomy of a Sandworm: A Deep Dive into the Shai-H...	Megg Sage
10:10 - 11:40	The Silent Tunneler: A Real-World Incident Respons...	Uriel Kosayev
12:25 - 13:05	North Korea's Zoo: Poaching for Gophers, Armadil...	Mauro Eldritch
12:10 - 14:10	Introduction to Reverse Engineering With Ghidra	Wesley McGrew
13:15 - 13:55	Return of Sedinho: Current situation and new tacti...	Josep Albors
14:05 - 14:45	Smart Contracts, Smarter Malware: Automating Recon...	Sai Sathvik Ruppa,Chris N...
14:55 - 15:35	The State of Decompiler Malware	Christopher Hernandez
14:10 - 17:25	The Achaean project-Trojan development for noobs	Leigh Gilbert
15:45 - 16:25	Vibe Check: Exploiting Developer Trust from Prompt...	Michael Chan
16:35 - 17:15	You Hold the Helm: Agentic LLM Workflows for Malwa...	Asher Davila,Lenin Alevsk...
Saturday		
10:45 - 11:25	Demystifying the Playboy RaaS	Gijs Rijnders
10:00 - 10:35	Cracking ValleyRAT: From Builder Secrets to Kernel...	Jiří Vinopal
10:10 - 12:10	Hostile Input: PDF Triage That Survives an Adversa...	Klaus Wunder
11:35 - 12:15	Haetae: An Agent to Takedown North Korean C2 Serve...	Nelson Colon
12:55 - 14:05	A hands-on hour with IDA: reverse-engineer a real...	David Rushmer
13:50 - 14:30	How to destroy a country	Lisandro Ubiedo,Leandro C...
13:05 - 13:45	Ropkit: Framework for Windows Kernel Code Executio...	Nathan Sawyer
14:40 - 15:15	The Permanent Threat: Analyzing Aeternum's Block...	Chris Navarrete,Sai Sathv...
14:10 - 16:50	An Intro to Mac Malware Analysis	Patrick Wardle
15:20 - 16:05	Leigh Trinity OTW	Leigh Gilbert
16:15 - 16:55	The AI Analysis Train is Leaving the Station: ALL...	Ryan "@rj_chap" Chapman

[Return to Index](#)

Maritime Hacking Village

Location: LVCCW Level 1 Hall 2 703 (Maritime Hacking Village) - [Map](#)

Home Page: <https://maritimehackingvillage.com/>

Sched Page: <https://maritimehackingvillage.com/dc34>

PDT Times	Title	speaker
Friday		
10:00 - 10:45	Maritime Hacking Village Policy Panel: Subsea Cabl . . .	Dr. Nina Kollars,Jason Vo . . .
11:30 - 12:15	Building the Humans Behind the Mission: Talent, Re . . .	Dr. Nina Kollars,Dr. Wand . . .
12:15 - 12:59	Maritime Hacking Village Policy Panel: Shadow Flee . . .	RADM John Mauger,Michael . . .
13:45 - 14:15	Drag, Drop, Deploy, Compromise: Why Trusted HMI En . . .	Jiwoon Yoo,TaeWoo Kim,Eun . . .
14:15 - 14:45	Scuttling Dashboards	Karan Sajnani
Saturday		
12:00 - 12:30	Please Place Your Electronic Devices in {Maritime} . . .	Jason Veara
12:30 - 12:59	Maritime Threat Hunting: What We Actually Find Whe . . .	Cliff Neve,Philip Acosta, . . .
16:30 - 16:59	LSTM Autoencoder Ensemble for NMEA 2000 Intrusion . . .	Anissa Elias,James Campbe . . .
16:00 - 16:30	Shipcrawler: Automated Maritime OSINT — From Ope . . .	Ahmed Nagi Nasr

[Return to Index](#)

Middle Easterns & Africans in Cyber Security (MEACS)

Home Page: <https://meacs.org/>

PDT Times	Title	speaker
Friday		
11:00 - 11:59	Logsquashing: Consolidating Relevant Events Logs a . . .	Ezz Tahoun
12:00 - 12:59	Once Upon a Prompt: Fairy Tales That Explain AI Se . . .	Sana Talwar
13:00 - 13:59	Nothing Wrong Here: Why AI Artifact Scanners Wave . . .	Amber Bennoui
14:00 - 14:59	The Agentic Free Pass: Does an Abliterated Backbon . . .	Karol Piekarski,Nishith S . . .
15:00 - 15:59	The New Horizons in Quantum and Space	Anshu Gupta
16:00 - 16:59	Defense in Depth for AI: Launching the AISECA Fram . . .	Amber Bennoui,Karol Pieka . . .
17:00 - 17:30	Condense, Contextualize, and Correlate: Optimize C . . .	Ezz Tahoun
17:00 - 17:59	What Got You Here Won't Get You There: Security in . . .	Amber Bennoui
Saturday		
10:00 - 10:59	From al-Kindi to DEF CON: The Middle Eastern and A . . .	Amber Bennoui,Ezz Tahoun
13:00 - 13:59	BewAIre: Detecting Malicious Pull Requests at Scal . . .	Andrew Krug
14:30 - 14:59	Condense Volumes, Connect Dots, Enrich Contexts: S . . .	Ezz Tahoun
14:00 - 14:59	The Hidden Data Supply Chain: How a SaaS Platform . . .	Sam Jadali
15:00 - 15:59	Agents of Chaos: A Field Guide to How Agentic AI G . . .	Amber Bennoui
17:30 - 17:59	The Autonomous SOC Blueprint: On-Premise ML & AI t . . .	Ezz Tahoun
17:00 - 17:59	MEACS Trivia, Games and Networking	
Sunday		
10:00 - 10:59	From Roots to Renaissance: The Rising Generation o . . .	Ezz Tahoun
12:00 - 12:30	The Dark Art of Alert Correlation: Extracting Atta . . .	Ezz Tahoun
12:00 - 12:59	Where the Authorization Boundary Goes in Agent Wor . . .	Mohamed Magdy AbuMuslim
13:00 - 13:59	MEACS Trivia, Games and Networking	

[Return to Index](#)

Misc

PDT Times	Title	speaker
Friday		
10:00 - 10:59	Coloring Reset	
12:00 - 12:59	From Disk Image to ATT&CK in One Binary — a Refe . . .	HUI Kwun Tai, Albert (4n6 . . .
12:00 - 12:59	Friendship Bracelets	
15:30 - 16:30	tAIrot Readings	
Saturday		
10:00 - 10:59	Coloring Reset	
12:30 - 12:59	Donating Bone Marrow: A Donor's First-Hand Experie . . .	
12:00 - 12:59	Friendship Bracelets	
13:30 - 14:30	Why Mandatory Age Verification Keeps Us All Less S . . .	Alexis Hancock,Kenyatta T . . .
15:30 - 16:30	Privacy's Defender with Women in Security and Priv . . .	Cindy Cohn,Alyssa Coley
Sunday		
10:00 - 10:59	Coloring Reset	
12:00 - 12:59	Friendship Bracelets	

[Return to Index](#)

Mobile Hacking Community

Home Page: <https://mobilehackingcommunity.com/>

Sched Page: <https://mobilehackingcommunity.com/schedule/>

PDT Times	Title	speaker
Friday		
10:00 - 17:59	Mobile Hacking - Informal CTF	
10:00 - 17:59	Mobile Hacking Community - Open	
10:00 - 10:45	Bypassing KYC Vendors on AI Times	Juan Urbano Stordeur,Juan . . .
11:00 - 11:59	AI finds and writes my Android exploits now	Ken Gannon /
12:15 - 12:45	Offensive Security from Your Pocket	Lukas Stefanko
13:00 - 14:30	Hacking Android Apps in a Structured Way	Sven Schleier
15:00 - 15:45	Mobile Security through Obscurity, from insecure c . . .	Juan Urbano Stordeur,Juan . . .
16:00 - 16:30	Leveraging Frida to Bypass Mobile Application Secu . . .	Jarrold Rizor
Saturday		
10:00 - 10:59	A Droidwork Orange: A Longitudinal Study of Androi . . .	Nicholas Miazso,Eleonora . . .
10:00 - 10:59	RedMatter: Let AI Write Your Cross-Platform Mobile . . .	Subho Halder
10:00 - 17:59	Mobile Hacking Community - Open	
10:00 - 17:59	Mobile Hacking - Informal CTF	
11:15 - 12:15	An Android voyage from Java to Smali with ASM	Ricardo Loura
12:30 - 12:59	Triage vs. Reality: Mobile Security Findings in Bu . . .	fr4vian
13:15 - 14:45	Hacking iOS Apps in a Structured Way	Sven Schleier
15:00 - 15:59	Beerus Framework – A New Mobile Framework Arises	João Pedro Tricta,Daniel . . .
Sunday		
10:00 - 13:59	Mobile Hacking Community - Open	
10:00 - 11:59	Mobile Hacking - Informal CTF	
11:30 - 11:59	IsMyPhonePwned: Analyzing Android/iOS Phones at Sc . . .	Desnos Anthony

[Return to Index](#)

Nix Vegas Community

Home Page: <https://nix.vegas/>

PDT Times	Title	speaker
Friday		
10:00 - 10:30	Nix Vegas Opening Ceremony	Daniel Baker,Morgan Jones . . .
10:30 - 10:59	Composable Systems with NixOS MicroVMs	Alex Decious
11:30 - 11:59	Running a homelab with NixOS	Aaron Honeycutt
13:00 - 13:45	Whose PR Is It Anyway?	
14:00 - 14:30	Relocatable Nix Binaries	Farid Zakaria
15:00 - 15:30	Everything is Nix when you squint hard enough	Jared
16:00 - 16:30	NixOS Workspaces	JB
16:45 - 16:59	Github Rate Limits Got You Down? FOD's Failing t . . .	Ethan Carter Edwards
17:00 - 17:59	Lightning Talks and Unconference	
Saturday		
10:30 - 10:45	How to piss off your Nix friends	Farid Zakaria
10:00 - 10:30	Nix Vegas Opening Ceremony	
10:45 - 10:59	Beholden to No One: The Nix Override Ladder	Daniel Baker
11:30 - 11:59	Compiling the World: A Binary Dataset Built from n . . .	Chris Connelly
13:00 - 13:45	Whose PR Is It Anyway?	
14:00 - 14:30	Nix Knows When the Agent Is Wrong	Jason Odoom
14:45 - 15:15	Securing Nix Builds using microVMs	Tristan Ross
15:30 - 16:30	Your Infrastructure Is a DAG: Manage It With Nix	Ethan Carter Edwards
16:30 - 16:59	Breaking the Chains of Cloud Giants: Building a Fu . . .	Maksim Kuskov,Mikhail Ili . . .
17:00 - 17:30	Lightning Talks and Unconference	
Sunday		
13:30 - 14:30	Unconference	
13:00 - 13:30	Nix Vegas Closing Ceremony	

[Return to Index](#)

Noob Community

PDT Times	Title	speaker
Friday		
10:00 - 17:59	TCM Security Labs	
10:00 - 17:59	Skillbit Labs	
10:00 - 17:59	SANS Institute NetWars Labs	
10:00 - 17:59	No Stupid Questions	
10:00 - 10:55	Noob Community - DEF CON 34 Opening Statements	
10:00 - 17:59	Kryptsec Labs	
10:00 - 17:59	Hack The Box DC Junior Ranger Program Challenge	
10:00 - 17:59	Arcanum Security Labs	
10:00 - 17:59	Mentoring and Career Advice	
10:00 - 13:50	Practical Cybersecurity Skills in an AI-Augmented . . .	James Stanger,Stephen Sch . . .
11:45 - 12:45	If I Were Eighteen Again: Career Advice for the AI . . .	Keith Hoodlet
11:00 - 11:30	Privilege Escalation: A Career Story	Ryan Bonner,Whit Taylor
13:30 - 13:59	OSINT: Zero To Hero	Mishaal Khan
13:00 - 13:15	Threatmaxxing Your Stakeholders while Mogging Your . . .	Eli Woodward
14:15 - 14:45	Day in the Life - Green Beret to AI Penetration Te . . .	Clayton Boozell
14:00 - 15:20	Beyond Heatmaps: Hands-On Cyber Risk Quantificatio . . .	Tony Martin-Vegue
15:30 - 15:45	Lessons Learned From A Decade of Resumes	Britt Kemp
15:30 - 16:59	Introduction to Web Exploitation	Roman Bohuk
15:00 - 15:15	The impact of CTF Write-Ups	Mathias Detmers
16:00 - 16:30	Building Your First Homelab	Stephen Glombicki
16:35 - 17:05	The Front Lines Need Detection Engineers : Would Y . . .	Kyle Barboza
Saturday		
10:00 - 17:59	Arcanum Security Labs	
10:00 - 17:59	Hack The Box DC Junior Ranger Program Challenge	
10:30 - 10:45	The importance of Networking in Cybersecurity comm . . .	Michael Lenz
10:00 - 10:15	Wanna Hack Space ? Why? Is it out of this world?	Henry Danielson Hankashyy . . .
10:00 - 11:20	Break Things, Learn Things: Hands-On Hacking for B . . .	Evolve Security Academy
10:00 - 17:59	Kryptsec Labs	
10:00 - 17:59	Mentoring and Career Advice	
10:00 - 17:59	No Stupid Questions	
10:00 - 17:59	TCM Security Labs	
10:00 - 17:59	Skillbit Labs	
10:00 - 17:59	SANS Institute NetWars Labs	
11:00 - 11:30	No One Makes It Alone - Community as the Ultimate . . .	Kristen Sanders
11:30 - 12:50	OASIS: Prompt to Pwn	Marshall Livingston
11:45 - 12:45	Gamifying the Matrix: a MITRE ATT&CK Video Game	Annie Meaney,Anne Drago
13:00 - 13:59	Getting Started in OT/ICS Cybersecurity	Mike Holcomb

PDT Times	Title	speaker
13:00 - 14:50	redStack: Boot-to-Breach Red Team Platform	Michael Ortiz
14:15 - 14:45	Privilege Escalation: Building a Cyber Career with . . .	Akanksha Raghvesh
15:00 - 15:59	Six Impossible Things Before Breakfast: Common Mis . . .	Brett Tolbert
15:00 - 16:59	AI Hacking for Noobs	Jason "jhaddix" Haddix,Ar . . .
16:15 - 16:45	Imposter Syndrome Is Distracting You From the Work . . .	Samantha Schwartz
Sunday		
10:30 - 11:30	Ctrl + Alt + Lead: Rebooting Cyber Culture with Hu . . .	Amanda Kollmorgan
10:00 - 10:59	Break Things, Learn Things: Hands-On Hacking for B . . .	Evolve Security Academy
10:00 - 13:59	Hack The Box DC Junior Ranger Program Challenge	
10:00 - 13:59	Arcanum Security Labs	
10:00 - 13:59	Mentoring and Career Advice	
10:00 - 13:59	Kryptsec Labs	
10:00 - 13:59	No Stupid Questions	
10:00 - 13:59	TCM Security Labs	
10:00 - 13:59	Skillbit Labs	
10:00 - 13:59	SANS Institute NetWars Labs	
11:45 - 12:15	So You Want to Be a Red Teamer? The Reality Behind . . .	Billy Giles
11:00 - 12:59	From Command Line to Center Stage: Hack Your Way t . . .	James McQuiggan
12:30 - 12:59	Be your own Agent: Career Journey and Advice from . . .	Meghan Jacquot
13:05 - 15:55	Noob Community - Conference Closing	

[Return to Index](#)

OSINT For Good Community

Home Page: <https://www.tracelabs.org/>

PDT Times	Title	speaker
Friday		
10:00 - 10:59	OSINT4Good: What it takes to find missing people	Angela Ramos,Kenny J,Bren . . .
10:00 - 17:59	OSINT4Good Community - DC NextGen Content	
10:00 - 17:59	FINDX OSINT Educational Series	
11:00 - 11:30	Q&A with the OSINT4Good Panel	Angela Ramos,Kenny J,Bren . . .
11:45 - 12:15	Welcome to OSINT4Good and Trace Labs	Nataly "someone_somewhere . . .
12:30 - 13:15	Geolocating Talent: How OSINT CTFs are Building To . . .	Ben "The Cyber Sensei" Cr . . .
13:30 - 14:30	Classical OSINT using AI (Actual Intelligence)	Bianca C. Ionescu/reconce . . .
14:30 - 14:59	Q&A with the Classical OSINT Using AI speaker	Bianca C. Ionescu/reconce . . .
15:30 - 16:30	Trace Labs L100: Search Party Basics	Sarah "scba" Miller
17:30 - 17:59	Tracelabs VM Installation Workshop	
17:00 - 17:30	Installing and Using the Tracelabs VM	Jeff "UltraSunshine" G
Saturday		
10:00 - 17:59	FINDX OSINT Educational Series	
10:00 - 17:59	OSINT4Good Community - DC NextGen Content	
10:00 - 10:59	Trace Labs L150: Case Walkthrough	Brent Louie
11:15 - 11:45	CTF Intro, Quick Guides, and Rule Review	Kenny J
16:00 - 16:59	OSINT Search party CTF Debrief	Trace Labs Staff
17:00 - 17:15	OSINT Search Party CTF Prize and Award Announcemen . . .	
17:15 - 17:59	OSINT4Good Sticker Swap	
Sunday		
10:00 - 13:59	OSINT4Good Community - DC NextGen Content	
10:00 - 13:59	FINDX OSINT Educational Series	
10:30 - 10:59	How to Profile an entire C-suite in 10 days	Sarah Muriel
11:00 - 11:15	Q&A with the "How to Profile an entire C-suite in . . .	Sarah Muriel
11:30 - 12:45	Disaster Intelligence - The past, present, and fut . . .	Matt Green
11:30 - 11:59	Disaster Intelligence - The past, present, and fut . . .	Matt Green
12:15 - 12:45	Practical Privacy Defenses for the Paranoid	Tina "Hek8te" Shakour
13:00 - 13:59	Building a Student-Led OSINT Program to Investigat . . .	Angela Ramos

[Return to Index](#)

OWASP Foundation

Home Page: <https://owasp.org/>

PDT Times	Title	speaker
Friday		
10:00 - 17:59	BadVR: Signals Everywhere a collaboration with XR . . .	Jad Meouchy,Suzanne Borde . . .
11:30 - 11:59	Spotlight: Choose Your Own Adventure with InfoSecM . . .	W. Martín Villalba
12:00 - 13:59	OWASP ISTG in Practice: A CTF-Style IoT Hacking & . . .	Piero "p33_p33_" Picasso, . . .
14:30 - 15:15	Defend zee clankers: OWASP AI Security Verificatio . . .	Jim Manico
14:00 - 15:59	Life Finds a Way: Secure Coding with OWASP ASVS	Eden Yardeni
15:15 - 15:59	Forged in fire: Malware Factory	Jon McCoy,Andra Lezza
16:00 - 17:59	OWASP Amass v5.0	Jeff Foley
17:30 - 17:59	AI Pentesting is not a Vibe Check	Ads Dawson
Saturday		
10:00 - 17:59	BadVR: Signals Everywhere a collaboration with XR . . .	Jad Meouchy,Suzanne Borde . . .
10:30 - 10:59	Spotlight: Choose Your Own Adventure with InfoSecM . . .	W. Martín Villalba
10:00 - 10:59	Let's Play! OWASP Cornucopia for Mobile Applicatio . . .	Sven Schleier
11:00 - 11:59	Oh hai! Meet Tanya "SheHacksPurple" Janca	Tanya "SheHacksPurple" Ja . . .
12:00 - 12:59	Oh hai! Meet Jason Haddix	Jason "jhaddix" Haddix
13:00 - 13:59	FTS Build it Yourself: cDc X OWASP X Veilid	Gibson,medus4,cdC & Veili . . .
14:00 - 15:59	Agents & Exploits: Hacking OWASP VWAD	Philippe "pilvar" Dourass . . .
16:00 - 17:59	Practical AI Security Assessments Using OWASP AISV . . .	Jim Manico
Sunday		
10:30 - 12:30	2001: Agentic Odyssey in Threat Modeling	Petra Vukmirovic
10:00 - 10:30	Spotlight: Choose Your Own Adventure with InfoSecM . . .	W. Martín Villalba
11:00 - 13:59	OWASP Chapter Meetup	
12:30 - 12:59	Source of Truth: A Field Guide for Deep Technical . . .	Carley "51nk0r5w1m" F . . .
12:00 - 12:59	Let's Play! OWASP Cornucopia Threat Modeling	

[Return to Index](#)

Packet Hacking Village

Location: LVCCW Level 3 W303-310 (Packet Hacking Village) - [Map](#)

Home Page: <https://www.wallofsheep.com/>

Sched Page: <https://www.phvillage.io/pages/dc34/>

PDT Times	Title	speaker
Friday		
14:30 - 15:30	Wiring the Harness: Orchestrating Frontier Models . . .	Tony Martin,Arie Haenel
Saturday		
13:00 - 13:59	Building Better Backdoors Than China	Khael Kugler
15:00 - 15:59	There's A Bug in My Boot! Finding Vulnerabilities . . .	Jared Stroud
16:00 - 16:59	Why Couldn't I See My Own Drone? Remote ID, ESP32s . . .	Will Hatzer,Charles Grow
17:00 - 17:59	Ghost Followers: Using AI to Unmask Fake LinkedIn . . .	Aiswarya Venkitesh

[Return to Index](#)

Payment Village

Location: LVCCW Level 2 W204-205 (Payment Village) - [Map](#)

Home Page: <https://www.paymentvillage.org/>

PDT Times	Title	speaker
Friday		
10:45 - 11:30	The Future of Payments: AI, Agentic Commerce and t . . .	Daniel Cuthbert,Leigh-Ann . . .
10:30 - 10:45	Payment Village Intro - What's Happening at the Vi . . .	
11:30 - 11:50	Introduction to Vulnerable ATM Badge	Vincent Sloan
11:00 - 11:20	A Real-Time Battle with a Card-Testing Adversary	Levi Schuck
12:00 - 12:45	Skimmers, Shimmers, and You	Aidan Quimby
13:30 - 13:59	It's a Payment Terminal. It's My Arcade. It's Ever . . .	Chiao-Lin Yu "Steven Meow . . .
13:00 - 13:20	Wall of Wallets Workshop (Intro to Wall of Wallets . . .	Dan Borgogno
14:00 - 14:45	How to Epically Fail Your PCI Assessment	Kevin Buck
15:00 - 15:45	Deepfake Detection Through Adversarial Research	Efim Boieru
16:00 - 16:45	Breaking BIOS in ATMs	Arnold Jared Morales Yepe . . .
Saturday		
10:30 - 10:45	Payment Village Intro - What's Happening at the Vi . . .	
11:00 - 11:20	Victim as a Service: Engaging with Trust-Based Sca . . .	Ariana Mirian
11:30 - 11:50	Introduction to Vulnerable ATM Badge	Vincent Sloan
12:00 - 12:59	Breaking PBKDF - Adversarial Cryptanalysis and Tec . . .	Ken Pyle
14:30 - 15:15	Deepfake Detection Through Adversarial Research	Efim Boieru
14:00 - 14:20	BNPL's Blind Spot: Exploiting Business Logic Flaws . . .	Furkan Fatih Demir
16:00 - 16:45	Compounding Interest: Exploiting the ATM Supply Ch . . .	Matt Burch
Sunday		
10:30 - 10:50	Wall of Wallets Workshop (Intro to Wall of Wallets . . .	Dan Borgogno
12:00 - 12:15	CAPTURE THE COIN - Announcement of the CTF Winners	

[Return to Index](#)

Physical Security Village

Location: LVCCW Level 1 Hall 2 601 (Physical Security Village) - [Map](#)

Home Page: <https://www.physsec.org/>

PDT Times	Title	speaker
Friday		
12:30 - 12:59	Introduction to RFID	Ege Feyzioglu,Karen Ng
12:00 - 12:30	Flow Like Water: Experiences from Physical Red Tea . . .	Michael "v3ga" Aguilar
15:30 - 15:59	Forensics of Covert Entry	Bill Graydon,Bobby Graydo . . .
16:00 - 16:30	The Door Was Already Open	Champ
Saturday		
11:00 - 11:59	No Entry: Badge Access Denial on Demand	Andrew Quill
13:30 - 13:59	FORTRESS Framework	Brad "Sno0ose" Ammerman
14:00 - 14:59	Clone to Pwn: Remote Badge Cloning with the Flippe . . .	Langston Clement,Dan Goga
16:00 - 16:59	Zero-Knowledge Unsaflok: The Unsaflok Saga Continu . . .	Ben Higgins,Aaron Tulino
Sunday		
10:00 - 10:30	Breaking In, Evil Style: A Guide to Scaring Your C . . .	Andrew Lebedinsky
11:00 - 11:59	Physical Security is not sexy which is bad for org . . .	Roger Egan
12:00 - 12:59	Travel Security: Viewing Risks Through the Eyes of . . .	Tim Roberts,Brent White

[Return to Index](#)

Policy @ DEF CON

Location: LVCCW Level 2 W210-211 (Policy Village) - [Map](#)

Home Page: <https://defcon.org/policy/>

Sched Page: <https://bsky.app/profile/defconpolicy.bsky.social/post/3mqhrqudiv22b>

PDT Times	Title	speaker
Friday		
10:00 - 10:59	Sovereign by Design, Vulnerable by Default	Devin Lynch,Haley Ring
10:00 - 10:59	Not Your Parents' Schoolhouse Rock: Getting Tech ...	Jeff Rothblum,Michael Fly ...
11:00 - 11:59	Morbidity and Mortality: Hackers, HIPAA, and a new ...	Christian Dameff,Jeff "r3 ...
12:00 - 12:59	Election Security in the Age of AI: Governance, Tr ...	Lester Godsey,William Gat ...
13:00 - 13:59	Connectivity as Control in the European High North	Szymon Skalski,Patricia V ...
13:00 - 13:59	The Cyber Crystal Ball: The Annual Policy @ DEF CO ...	Matthew Wein,Bruce Schnei ...
14:00 - 14:30	The Liability Stack: When Code Becomes Conduct	Carole House
14:00 - 15:30	Strengthening the CVE Ecosystem (Seating is limite ...	John Banghart,Elizabeth E ...
15:30 - 16:30	Privacy's Defender: How Hackers Protected the Inte ...	Cindy Cohn
15:30 - 16:30	When AI Finds Everything: Vulnerability Policy for ...	Alec Summers,Lindsey Cerk ...
16:00 - 16:30	Building a State Wide VDP: Lessons from Maryland's ...	01dbae
16:30 - 16:59	Legally Hacked: how countries decide when security ...	Katharina "Kat S" Sommer
16:30 - 17:59	Filibuffer Overflow: Hackers Stage A Congressional ...	Katherine Pratt,Jeff Roth ...
Saturday		
10:00 - 10:59	Whose Agent Is It Anyway? Agency, Authorization, a ...	Andreas Kaltsounis,Jacob ...
10:00 - 10:59	Journey to Create an All-state Cybersecurity Plan ...	Craig "jafo" Buchanan
11:00 - 11:59	From Policy to Prod: How a Frontier AI Lab Enforce ...	Grant Versfeld,David "0xd ...
12:30 - 13:30	Privacy You Inherit: How Cultural History Writes t ...	Tati
12:00 - 12:59	Europe's Expanding Role in Global Vulnerability ...	Nuno Rodrigues Carvalho,R ...
13:30 - 13:59	The Subverted Hacker	Robert "zizkill" Shala
13:00 - 13:59	Surprise Session - Check Hacker Tracker	
14:00 - 14:30	The best of three bad ideas? Ransomware taxes in l ...	Joe Uchill
14:30 - 15:30	From Disclosure to Defense: Rebuilding Vulnerabili ...	Lindsey Cerkovnik,John Ba ...
15:30 - 15:59	Assume Breach, But For Real: Rewriting Infrastruct ...	Travis Berent,Adam Hickey
16:00 - 16:59	Securing the Safety Net: Why Healthcare Cybersecur ...	Sahan Fernando,James Bowi ...
17:00 - 17:30	AI Safety Theater: What the RAISE Act Regulates ...	Joshua Marpet
17:00 - 17:59	The Closing Window: Governing Agentic AI Security ...	Taylor Roberts,Mitch Herc ...
Sunday		
11:00 - 11:59	Strategic Resistance: How a Global Network is Figh ...	Michael Brennan,Nadine Fa ...
12:00 - 12:30	Inference in the Infrastructure: Developing NIST A ...	Raymond Sheh,Martin Stanl ...
12:30 - 13:59	Tactical Advocacy: Panel & Peer Sessions with EFF	Thorin Klosowski,Cooper " ...

[Return to Index](#)

Quantum Village

Location: LVCCW Level 1 Hall 2 605 (Quantum Village) - [Map](#)

Home Page: <https://quantumvillage.org/>

PDT Times	Title	speaker
Friday		
16:30 - 16:59	Covert Quantum Computing - a new quantum security . . .	Evan Anderson
17:00 - 17:30	Q-Day - the Early Years...	Konstantinos Karagiannis

[Return to Index](#)

Queercon Community

Home Page: <https://queercon.org/>

PDT Times	Title	speaker
Friday		
11:00 - 11:59	Trans Townhall	
12:00 - 12:59	QueerCon Opening Meet and Greet	
13:00 - 13:59	Non-Binary/Gender Non-conforming Meetup	
14:00 - 14:59	Women Loving Women Meetup	
15:00 - 15:59	Furs and Kinksters Meetup	
Saturday		
11:00 - 11:59	Polycon	
12:00 - 12:59	Trans Meetup	
13:00 - 13:59	Ace/Aro Meetup	
14:00 - 14:59	Own the con	
15:00 - 15:59	Men Loving Men Meetup	

[Return to Index](#)

Radio Frequency Village

Location: LVCCW Level 1 Hall 1 409 (Radio Frequency Village) - [Map](#)

Home Page: <https://rfhackers.com/>

PDT Times	Title	speaker
Friday		
10:30 - 12:25	RF CTF Kick Off Day 1	RF Hackers
10:00 - 17:59	Radio Frequency Village Events	
12:30 - 13:25	Let's BLESPl0.it the world together - introducing . . .	Slawomir Jasek
13:30 - 14:25	Fox Hunting - Finding Rogue Access Points in the C . . .	Eric Escobar
13:00 - 13:59	Running your own LTE network for fun and profit??? . . .	Lozaning
14:30 - 14:55	Security Vulnerabilities in SATCOM Devices	Aumkareshwar DS
15:30 - 16:25	AI-assisted RF Hacking with GNU Radio	Erwin Karincic (Dollarhyd . . .
15:00 - 15:25	Hack the Planet (not ours)	Abraxas3d
16:30 - 16:55	Supertooth: Wideband Bluetooth Observation with a . . .	Dalton Cox
16:00 - 16:30	Practical Guidance for RF Researchers: Experiment . . .	Andy Hendrickson
17:00 - 17:55	WiFi Shuriken: A New Architecture For High Perform . . .	CoD_Segfault
17:00 - 17:59	Latest News in the Proxmark World	Iceman
Saturday		
10:30 - 12:25	RF CTF Kick Off Day 2	RF Hackers
10:00 - 17:59	Radio Frequency Village Events	
12:30 - 13:25	Neotropolis: The Making of the Railgun Trackers	John O'Connor
13:30 - 13:55	This is a Test: Vibe Hacking LTE Cell Broadcast fo . . .	XtraRaj
14:00 - 14:55	RASM: A State Machine Methodology for RF Security . . .	Smriti Gaba
15:00 - 15:55	Drone ID on the Wire: RF Detection, Spoofing, and . . .	Greg Albrecht
16:00 - 16:25	Yes, it runs Doom: over the air gaming on a bladeR . . .	max
16:30 - 17:25	I'm Not Special, and You Can Too! A journey into R . . .	Hampspiced
17:30 - 17:55	\$750 and a Weekend: Passive Direction Finding Acro . . .	K0YTL
Sunday		
10:00 - 11:55	WarDriver Meetup	
10:00 - 13:59	Radio Frequency Village Events	
12:00 - 12:55	RF CTF and World Wide War Drive Outbrief	RF Hackers

[Return to Index](#)

Recon Village

Location: LVCCW Level 1 Hall 2 501 (Recon Village) - [Map](#)

Home Page: <https://reconvillage.org/>

Sched Page: <https://reconvillage.org/reconvillage-2026-defcon-34/talks>

PDT Times	Title	speaker
Friday		
10:00 - 12:30	Hands-On Supply Chain Recon & Vendor Risk Mapping	Dhiyaneshwaran Balasubram . . .
10:00 - 23:59	TrackTheFugitive Contest	
10:00 - 23:59	Live Recon Contest	
10:45 - 11:30	InQuorigible: Quora in Missing Persons OSINT	Miranda Tedholm
11:00 - 16:59	GE(O)SINT Contest	
12:40 - 15:10	Threat Actors: Gotta Catch 'Em All	Marcelle Lee,Will Thomas
13:00 - 13:45	OSINT Is Still a Thinking Game: Surviving AI Witho . . .	Nico Dekens
15:30 - 17:59	BBOT: Automating the OSINT Kill Chain with a Singl . . .	Mark Gaddy
16:30 - 16:59	Groking the Kill Chain	Anthony Russell
Saturday		
10:00 - 12:30	Hunting the Contagious Trader Delivery Network	Alessandra Rizzo,Ariel Ro . . .
11:00 - 16:59	GE(O)SINT Contest	
12:00 - 17:59	TrackTheFugitive Contest	
12:40 - 15:10	The Hard Part of ASM: Ownership Attribution	Jeff Foley
12:00 - 13:59	Live Recon Contest	
13:30 - 13:59	Your OpSec Is Showing	Fae Blu3Bird" Carlisle
13:00 - 13:30	Tag, You're It: Physical Tracking Tech, Defense, . . .	Eddie Miro
15:20 - 17:50	Vibe Coding Your Way to a Fully Functional Open-So . . .	Lenin Alevski
15:00 - 15:30	The Breach Is Over. The Exposure Is Not	Kumar Ashwin,Anant Shriva . . .
15:30 - 15:59	Cl0p ^_- Til You Drop - 6 years, 9 Campaigns, 7 0- . . .	Eli Woodward
16:00 - 16:59	Live Recon Contest — Final Presentations	
17:30 - 17:59	Total Recon: How We Discovered 1000s of open Agent . . .	Avishai Efrat,Roey Ben Ch . . .
17:30 - 17:59	There Is No Internet: Cross-Domain Recon of all 4. . . .	John McCary
17:00 - 17:30	CyberKB: When Your AI Copilot Runs the Recon, Craw . . .	Suriya Prasath S,Chandru . . .
Sunday		
10:00 - 10:45	Ghost in the Hiring Machine: How to Spot Fake Pers . . .	Michael Reimsbach,Rishi " . . .
10:45 - 11:30	Living Off Someone Else's Inference	Redon Gashi,Armend Gashi
12:00 - 12:30	Recon on Trial: The OSINT Operator's Legal Playboo . . .	David Cass
12:30 - 12:59	Building Hackbots	Jason "jhaddix" Haddix

[Return to Index](#)

Red Team Village

Location: LVCCW Level 1 Hall 1 309 (Red Team Village) - [Map](#)

Home Page: <https://redteamvillage.io/>

Sched Page: <https://redteamvillage.io/schedule>

PDT Times	Title	speaker
Friday		
10:00 - 17:59	From Kiosk to Domain Compromise: Learning to Walk . . .	Ezra Woods, Mike Manrod, Sp . . .
10:00 - 17:59	BloodHound Quest	Hugo van den Toorn
10:00 - 11:59	Post-Exploitation of the Desktop with JS-Tap	Drew Kirkpatrick
10:00 - 11:59	Red Team Express	Cody Spooner
10:00 - 11:59	Zero Signal: Operating Where Defenders Can't See	Gowthamaraj Rajendran
10:00 - 11:59	Falco Hunt: Evading Runtime Detection in Kuberne . . .	Michael Reimsbach
10:00 - 10:59	Opening Panel - "Is Red Teaming Dead?"	Ads Dawson, Ben "NahamSec" . . .
10:00 - 10:59	The Entropy Illusion: High-Speed Cracking on a Bud . . .	Chris Claunch
10:00 - 11:59	RFID Bootcamp: Unleashed!	Evan Cook
11:00 - 11:59	Trusted Launcher, Untrusted Code: Weaponizing AppL . . .	Nathan Sawyer
11:00 - 11:59	COM Hijacking Voodoo: Tradecraft, Detection Blind . . .	Nikos "nickvourd" Vourdas
11:00 - 11:59	Exploiting Private 5G: Unauthenticated Access to D . . .	Aumkareshwar DS
12:00 - 13:59	Burning Redirectors Before Blue Team Does	Mohamed AbuMuslim, Saad Na . . .
12:00 - 13:59	From Application Telemetry Exposure to Cross-Servi . . .	Chirag Savla, Raunak "Trou . . .
12:00 - 13:59	Web Hacking Bootcamp	Emma Latuszek
12:00 - 13:59	Your Passkeys Won't Save You: Conditional Access B . . .	Doug Mooney, Jared Dobbela . . .
12:00 - 12:59	macOS Doesn't Get Malware...Until It Does	Zoziel Freire
12:00 - 12:59	BloodHound OpenGraph Crash Course	JD D
13:00 - 13:59	Shapeshifting C2: Applying DAITA Traffic Shaping t . . .	Rafael Felix
13:00 - 13:59	One Request to Rule Them All	Corey Ball
13:00 - 13:59	BloodHound OpenGraph: Six Degrees of Everything	Rohan Vazarkar, Wes Miller
14:00 - 15:59	Cloud-Native C2: Weaponizing Trusted Infrastructur . . .	Dhiraj Mishra
14:00 - 15:59	Quality over Quantity: How to Publish CVEs that Ac . . .	Natan Morette
14:00 - 15:59	Automated Mythic Deployment with Gaia	Shad Brown
14:00 - 15:59	Social Engineering With Reel	James Williams
14:00 - 14:59	Microsoft and Amazon are my Favorite C2 Providers	Robert Pimentel
14:00 - 14:59	Extension Hollowing: Abusing Chrome's Extension Tr . . .	Gordon Long
15:00 - 15:59	Trust the Pipeline, Lose the Kingdom: Hands-On Clo . . .	Shane Young
15:00 - 15:59	LLM-Coached Red Team Tactics to Attack Zero Trust	Rudy Ristich, Vijay Anand
16:00 - 17:59	EvilEssid: Evading Wireless Intrusion Prevention S . . .	Miguel Fernandez
16:00 - 17:59	redStack: Boot-To-Breach Red Team Platform	Michael Kim, Michael Ortiz
16:00 - 17:59	Haetae: An Agent to Takedown North Korean C2 Serve . . .	Mauro Eldritch, Nelson Raf . . .
16:00 - 17:59	Praetor: An OPSEC Exposure Advisor for Empire Oper . . .	Andrea Brosio, Ariz Sorian . . .
16:00 - 16:59	Trust Me, Bro: A field guide to Windows Authentico . . .	Fagan Afandiyev
16:00 - 16:59	Network Implants: Lessons Learned Building Reliabl . . .	Hassan Mohamad

PDT Times	Title	speaker
Saturday		
10:00 - 11:59	From Path Traversal to Domain Credentials in 90 Seconds	Mike Lisi
10:00 - 11:59	PMTCT: One-Click RCE and Persistent Exfil in AI Code	Ahmet Furkan Aydogan
10:00 - 11:59	MCP Servers: The Next Enterprise Attack Surface	Apoorwa Joshi, Justin Dray
10:00 - 11:59	Hands-On Autonomous Pentesting with Pentest Copilot	Dhruva Goyal, Sitaraman Sundar
10:00 - 10:59	Inside the Red Team Cabal: A Decade of Lessons from the Trenches	Jason Strange, Wes Thurner
10:00 - 11:59	Living Off the Vault	Alexandru Uifalv, Jennifer
10:00 - 11:59	Pyramid of Pain-Red Team (Human and Technical Fric	Frank Victory
11:00 - 11:59	DPAPI Is Not a Boundary: A Full Infostealer Kill Chain	Filipi Pires
11:00 - 11:59	The Authentic Operator: Social Engineering Through	Joanna
12:00 - 13:59	Ouroboros Attack! Recursive AI-Assisted 0-Day Hunt	Mehmet Önder Key, Temel D
12:00 - 13:59	Command & Conquer: Hands-on C2 Primer with Mythic	Logan MacLaren
12:00 - 13:59	Building Hackbots	Jason "jhaddix" Haddix, Ry
12:00 - 13:59	Red Teaming Kubernetes: From App-Level CVEs to Full	Lenin Alevski
12:00 - 12:59	Agentic AI Supply chain Vulnerability lab	Aamiruddin Syed, N A
12:00 - 12:59	The Protocol-Native Adversary: Full-Spectrum ICS S	Blessen Thomas, Javier Her
13:00 - 13:59	You Can't Block My C2 — It's Your Google Calendar	Nishant Tayade
13:00 - 13:59	Stop Chasing Domain Admin: Designing Red Team Exer	Billy Giles
14:00 - 15:59	Crawlee - Improving crawling with an LLM	Daniel Goldberg
14:00 - 15:59	Living Off Someone Else's Inference	Armend Gashi, Redon Gashi
14:00 - 15:59	AIMARU C2: The New Era of LotL (MCP AI-Driven C2)	Mario Lobo
14:00 - 15:59	BloodBash: Lightweight CLI Python BloodHound Alter	Anthony Russell
14:00 - 14:59	Turning Keys and Opening Doors: Leveraging AI Hype	Will Alexander
14:00 - 14:59	Chaining Credentials Through the AI Infrastructure	Nathan Keys
15:00 - 15:59	Requiem for the Decommissioned: When Dead Hosts Bi	Yekaterina Shevchenko
15:00 - 15:59	Breaking MCP Trust Boundaries: Cross-Server Author	Yevhen Pervushyn
16:00 - 17:59	The Quantum Mechanic: Attacking all the clouds	Moses Frost
16:00 - 17:59	Evading EDR in ATM	Arnold Jared Morales Yepe
16:00 - 17:59	MalSkill: Weaponizing AI Agent Skills for Persistence	Nur Gucu
16:00 - 17:59	Writing Production-Grade Exploits in go-exploit	Landon Rice
16:00 - 16:59	Control + C = Control Me	Andrew Griess
16:00 - 16:59	OSINT for Hackers Redux	Lee McWhorter, Sandra Stib
17:00 - 17:59	Below the Threshold: Real-World APT Tradecraft for	Jonathan Coradi, Oliveira
Sunday		
10:00 - 14:59	Attack Campaign in VR	James Rice
10:00 - 11:59	Tokens and PRT: Advanced Attacks and Persistence i	Elzer Pineda, Jose Rivas
10:00 - 11:59	0-Day Hunting Table: Come Join the Vulnpocalypse	Chris Haller
10:00 - 11:59	Evil Is Always a Bad Stylist: .NET Obfuscation wit	Alexander Rodchenko, Ashle
10:00 - 10:59	Beyond NPPSPY: Harvesting Credentials via Windows	Sohail Saha
10:00 - 10:59	Beyond the Flag: How CTF Players Become Product Se	Drew Thompson, Monish Alur
10:00 - 10:59	Direct Network Access for Command and Control	Andrew Rioux
11:00 - 11:59	Living Off WebView2: Turning Microsoft's Browser	Murilo Caixeta
11:00 - 11:59	Commit, Push, Compromise: Attacking Modern GitHub	Andrew Buchanan, Max CM

PDT Times	Title	speaker
12:00 - 13:59	Do you feel in control? Analysis of AWS CloudContr . . .	Bleon "gl4ssesbo1" Proko
12:00 - 13:59	From Buffer Overflow to Blackout: Chaining Attacks . . .	Fernando Mengali,Thiago C . . .
12:00 - 13:59	The Air Is Hostile: RF Trust Assumptions in Modern . . .	Mitch Breton
12:00 - 13:59	Living Off the IDE: From Initial Access to Covert . . .	Edo Maland
12:00 - 12:59	Agenthound: Mapping Multi-Hop Credential Chains Ac . . .	Adithyan Arun Kumar
12:00 - 12:59	Breaking and Defending NEURO: Hands-On AI Stack At . . .	Jason Ludwig
13:00 - 13:59	M0us3: A Lightweight, Multi Session C2 Framework w . . .	Aryan Jogia
13:00 - 13:59	Hacking the Human-in-the-Loop	Alexander "Zombie",Lee Mc . . .
14:00 - 14:59	beacon injected with HOOKCHAIN 2026	Arnold Jared Morales Yepe . . .
14:00 - 14:59	Ghost in the Water: Simulating a Nation-State PLC . . .	Blessen Thomas,Javier Her . . .
14:00 - 14:59	DFMI: Weaponizing MSI Installers for Fileless Code . . .	Anıl Çelik

[Return to Index](#)

Scambait Village

Location: LVCCW Level 1 Hall 1 208 (Scambait Village) - [Map](#)

Home Page: <https://teamtda.org/>

PDT Times	Title	speaker
Friday		
10:00 - 17:59	Open Q&A	
10:00 - 17:59	KSCM Scambait Radio	
11:30 - 13:59	Live Calls Workshop	
14:00 - 17:59	Live Call Listening	
Saturday		
10:00 - 17:59	Open Q&A	
10:00 - 17:59	KSCM Scambait Radio	
12:30 - 13:59	Scammers Don't Discriminate	DolphinVG
14:00 - 15:30	Creator Talk with RinoaPoison & VanHelen	RinoaPoison,VanHelen
15:30 - 16:59	Creator Drop-In	
Sunday		
10:00 - 15:59	KSCM Scambait Radio	
10:00 - 15:59	Open Q&A	
10:00 - 13:59	Scambait Bingo	

[Return to Index](#)

Social Engineering Community Village

Location: LVCCW Level 3 W317-319 (Social Engineering Community Village) - [Map](#)

Home Page: <https://www.se.community/>

Sched Page: <https://se.community/schedule/>

PDT Times	Title	speaker
Friday		
08:45 - 08:59	Village Greeting	
08:30 - 17:59	Social Engineering Community Village - Open Hours	
10:00 - 11:30	Pickpocketing for Red Teamers: A Hands-On Experien . . .	pradameinhof
12:00 - 12:59	Improv	
12:00 - 12:59	Zero Day Hire: Can You Spot the Spy?	Michael Reimsbach,Rishi " . . .
13:30 - 14:30	Zero Day Hire: Can You Spot the Spy?	Michael Reimsbach,Rishi " . . .
15:30 - 16:59	SE Improv	Bryan,Kevin
16:00 - 17:59	Cold Calls	
Saturday		
10:15 - 13:15	Battle of the Bots: Vishing Edition	
10:00 - 17:59	Social Engineering Community Village - Open Hours	
10:00 - 10:59	Social Engineering 101: The Four Psychological Bac . . .	Brian Brushwood
11:30 - 12:30	Social Engineering 101: The Four Psychological Bac . . .	Brian Brushwood
13:30 - 14:59	Hook, Line & Pretext Workshop: Crafting Effective . . .	Jenn,JC
14:00 - 14:30	For Prompt Injection, Press 1: Hacking AI Voice Ag . . .	Willie Zhang
14:30 - 14:59	The Sherlock Holmes Social Engineering Playbook	Elizabeth Rasnick
15:00 - 15:30	A Framework for Evaluating AI-Enabled Social Engin . . .	Fred Heiding
15:30 - 15:59	What Scammers Know That Social Engineers Don't: Th . . .	Megan Squire
15:30 - 17:30	2027 SECVC Pre-Qualification Round	JC,Snow
16:00 - 16:30	Wolfmasking: Teaching Everyday Defenders to Think . . .	Brian Brushwood
16:30 - 17:59	Cold Calls	
Sunday		
10:30 - 11:30	2027 SECVC Pre-Qualification Round - LIVE CALLS	
10:00 - 12:30	Social Engineering Community Village - Open Hours	
11:30 - 12:30	Cold Calls	

[Return to Index](#)

Social Gatherings/Events

Home Page: <https://defcon.outel.org/dcwp/dc34/activities/pge/>

PDT Times	Title	speaker
Wednesday		
11:00 - 17:15	The Unofficial DEF CON Shoot	
17:00 - 07:59	Linecon	
18:30 - 21:30	DC713 and DC281 - 8th Annual DEF CON Texas Groups . . .	
Thursday		
06:00 - 07:59	Defcon.run	
08:00 - 18:59	Human Registration Open	
08:00 - 17:59	Merch (formerly swag) Area Open -- README	
10:00 - 18:59	Music - SomaFM	
10:00 - 16:59	Ham In A Day Class	
12:00 - 12:59	Friends of Bill W	
15:00 - 20:59	Toxic BBQ	
17:00 - 17:59	Friends of Bill W	
18:00 - 19:59	Operator, Please Hold - DCG Social	
18:00 - 19:59	Exploit Your Own Story	Charel "1C0nur3r" Morris
18:30 - 23:30	Welcome Party at The Industrial	
19:00 - 19:59	Music - Genre: House	mattrix
19:00 - 21:59	DC702 Meetup	
20:00 - 20:59	Music - Genre: Electro House	Archwisp
21:00 - 21:59	Music - Genre: Breakbeats	PatAttack
21:00 - 23:59	Conference Planners Meetup	
22:00 - 22:59	Music - Genre: Breakbeats	Ice tre Normal
23:00 - 23:59	Music - Genre: Techno	Scotch and Bubbles
Friday		
00:00 - 00:59	Music - Genre: Techno	dotornot
06:00 - 07:59	Defcon.run	
06:00 - 10:59	15th Cycleoverride Bike Ride at DEF CON	
08:00 - 18:59	Human Registration Open	
08:00 - 17:59	Merch (formerly swag) Area Open -- README	
10:00 - 16:59	Malysis: A Bare-Metal RAM Enclave for Malware Anal . . .	Yannick LaRue,Samuel B. G . . .
10:00 - 16:59	Malysis: A Bare-Metal RAM Enclave for Malware Anal . . .	Yannick LaRue,Samuel B. G . . .
10:00 - 18:59	Music - SomaFM	
11:00 - 11:59	Book Signing - Nicholas DeMeo	Nicholas DeMeo
11:00 - 11:59	Book Signing - Christopher DeCarmen	Christopher DeCarmen
12:00 - 12:59	Friends of Bill W	
13:00 - 13:59	Book Signing - Brandy Smith	Brandy Smith
13:00 - 15:59	Free Ham Radio License Exams	

PDT Times	Title	speaker
14:00 - 14:59	Book Signing - Garrett Gee	Garrett Gee
14:00 - 15:59	Book Signing - Laura Scherling	Laura Scherling
14:00 - 15:59	Hacker Book Club Discussion	
15:00 - 15:59	Book Signing - Ted Harrington	Ted Harrington
15:00 - 16:59	Book Signing - Avinash Majeti	Avinash Majeti
16:00 - 16:59	Book Signing - Avinash Majeti	Avinash Majeti
16:00 - 17:59	Queercon Mixer	
16:00 - 18:59	Atlanta Metro Meetup (DC404/DC678/DC770/DC470)	
17:00 - 17:59	Friends of Bill W	
18:30 - 20:30	Policy Mixer Happy Hour	
18:00 - 19:59	Exploit Your Own Story	Charel "1C0nur3r" Morris
19:00 - 19:59	Music - Genre: Goth / Industrial	Daemon Chadeau
19:00 - 00:59	BlanketFort Con	
19:00 - 21:59	Lawyers Meet	
19:00 - 22:59	Social Engineering Community Village Party	
19:00 - 21:59	The KEVOPS Sellout Pool Party II: Sponsored by Zyn	
20:00 - 21:59	Hacker Jeopardy	
20:00 - 20:59	Music - Genre: Goth / Industrial	DJ Scythe
20:00 - 23:30	Women, gender non-conforming and non-binary meetup . . .	
20:00 - 23:59	Movie Night	
20:00 - 00:59	Hacker Karaoke	
21:00 - 00:59	Arcade Party	
21:00 - 21:59	Music - Genre: Nerdcore	Ohm-I
21:00 - 00:59	BIC R00T ACCESS 2026	
21:00 - 00:59	Day of the Dead Hacker Party	
22:00 - 23:59	Whose Slide Is It Anyway?	
22:00 - 00:59	SecKC the WHOLE WIDE WORLD	
22:00 - 22:59	Music - Genre: House	Skittish & Bus
22:00 - 00:59	Slopcon	
23:00 - 23:59	Music - Genre: Techno	TRIODE
Saturday		
00:00 - 00:59	Music - Genre: Trance	AfterGlow
06:00 - 07:59	Defcon.run	
09:00 - 18:59	Human Registration Open	
09:00 - 15:59	Merch (formerly swag) Area Open -- README	
10:00 - 18:59	Music - SomaFM	
11:00 - 12:59	Book Signing - Aamiruddin Syed	Aamiruddin Syed
11:00 - 11:59	Book Signing - Cindy Cohn	Cindy Cohn
11:00 - 16:59	Free Ham Radio License Exams	
12:00 - 12:59	Book Signing - Laura Scherling	Laura Scherling
12:00 - 12:59	Friends of Bill W	
13:00 - 13:59	Book Signing - Cindy Cohn	Cindy Cohn
13:00 - 13:59	Book Signing - Christopher DeCarmen	Christopher DeCarmen

PDT Times	Title	speaker
14:00 - 14:59	Book Signing - Garrett Gee	Garrett Gee
14:00 - 14:59	Book Signing - Brandy Smith	Brandy Smith
15:00 - 15:59	Book Signing - Mark Foudy	Mark Foudy
15:00 - 16:59	DCG New England Meetup	
16:00 - 16:59	Book Signing - Thomas Wilhelm	Thomas Wilhelm
16:00 - 16:59	Book Signing - Avinash Majeti	Avinash Majeti
16:00 - 17:59	Queercon Mixer	
17:00 - 17:59	Friends of Bill W	
18:00 - 20:59	10 years of K-rad (Hackers.Town Party)	
18:00 - 19:59	+61: the Australian Embassy	
18:00 - 22:59	2nd Annual Spades Night & Uno Tournament	
19:00 - 19:59	Music - Genre: Dubstep	ZipZapZop
19:00 - 20:59	DCNextGen Party!	
20:00 - 21:59	Hacker Jeopardy	
20:00 - 20:59	Music - Genre: Drum & Bass	RELAY
20:00 - 23:59	Movie Night	
20:00 - 00:59	Hacker Karaoke	
21:00 - 00:59	GOTHCON	
21:00 - 21:59	Music - Genre: Nerdcore	Dual Core
21:00 - 00:59	Front Man's Fête: An Octopus Game Party (includin . . .	
21:00 - 00:59	Party Line (Call Center Village Party)	
21:00 - 00:59	VETCON 2026 PARTY	
21:00 - 00:59	Illuminati Party	
22:00 - 00:59	Kayos Klub	
22:00 - 22:59	Music - Genre: Drum & Bass	Miss Jackalope
23:00 - 23:59	Music - Genre: Drum & Bass	Syntax + Luna
Sunday		
00:00 - 00:59	Music - Genre: Drum & Bass	DJ XORAC
06:00 - 07:59	Defcon.run	
09:00 - 11:59	Human Registration Open	
10:00 - 14:59	Music - SomaFM	
11:00 - 12:59	Free Ham Radio License Exams	
12:00 - 12:59	Friends of Bill W	
22:30 - 01:59	DEF CON After party @ LIV Fontainebleau	

[Return to Index](#)

Telecom Village

Location: LVCCW Level 3 W321 (Telecom Village) - [Map](#)

Home Page: <https://telecomvillage.com/>

PDT Times	Title	speaker
Friday		
10:20 - 10:59	A 5G Digital Twin CTF for Hacking Carrier-Grade In . . .	Siva Sareddu,T -Mobile CT . . .
10:00 - 10:20	Telecom Village Inauguration	Pankaj Sontakke
11:00 - 12:30	SOC Threat Hunting in Practice	Akib Sayyed
12:30 - 13:15	Poor Man's Mythos: Signal Siege: Agentic Exploit C . . .	Omer Farooq
14:15 - 14:59	Protecting Humans at Machine Speed - Engineering A . . .	Arvind Singh
15:30 - 15:59	AI vs AI: Securing Telecom in the Era of Autonomou . . .	Rohini,Pankaj Sontakke,Wi . . .
15:00 - 15:30	SIM Card Strikes Back: Telecom Threats & SOC Detec . . .	Zibran Sayyed
16:00 - 16:30	Nation State Obfuscation Networks	Will Thomas
16:30 - 16:59	Telecom Village CTF Closure	
17:00 - 17:59	Telecom Village Open Forum: Talks & Workshops: Rev . . .	
Saturday		
10:00 - 10:59	A 5G Digital Twin CTF for Hacking Carrier-Grade In . . .	T -Mobile CTF Team
11:45 - 12:30	From ONT to STB: Detecting IPTV Attack Chains in t . . .	Zibran Sayyed
11:00 - 11:45	Threats in Space: The Dangerous Rise of GNSS Attac . . .	Isabel Manjarrez
12:30 - 12:59	Signaling Sabotage: Why 100% Compliance is 0% Secu . . .	Vinod Shrimali
14:15 - 14:45	From Zero-Day to Zero-Hour: Rethinking Telecom Def . . .	Arvind Singh
14:00 - 14:15	Signal Hijacked: How Mobile Networks Became Phishi . . .	Sindhura Kona
15:45 - 16:45	Industry Challenges & SOC Reality	Vinod Shrimali
16:45 - 16:59	Telecom Village CTF Closure	
17:00 - 17:59	Telecom Village Open Forum: Talks & Workshops: Rev . . .	
Sunday		
10:20 - 13:59	Telecom Village CTF	T -Mobile CTF Team
14:00 - 14:15	Telecom Village CTF Awards Ceremony	

[Return to Index](#)

The Diana Initiative

Home Page: <https://www.dianainitiative.org/home>

PDT Times	Title	speaker
Friday		
10:10 - 10:20	IOT Village Tour	
10:20 - 10:30	Quantum Village Tour	
10:30 - 10:40	AppSec Village Tour	
10:40 - 10:50	Robot Hacking Community Tour	
10:50 - 10:59	Physical Securty Village Tour	
10:00 - 01:59	Quiet Room	
10:00 - 11:59	Hacker Runway Crafting Time	
11:00 - 11:10	Ham Radio Village Tour	
11:10 - 11:20	Packet Hacking Village Tour	
11:20 - 11:30	Mobile Hacking Tour	
11:30 - 11:40	Maritime Hacking Village Tour	
11:40 - 11:50	HHV/SSV Tour	
11:50 - 11:59	ICS Village Tour	
12:00 - 12:10	DEF CON Academy Tour	
12:50 - 12:59	DDoS Community Tour	
12:40 - 12:50	Call Center Tour	
12:30 - 12:40	Car Hacking Village Tour	
12:20 - 12:30	Cryptocurrency Village Tour	
12:10 - 12:20	DC Maker's Community Tour	
12:00 - 12:59	The Diana Initiative - Open time	
13:10 - 13:20	Telecom Village Tour	
13:00 - 13:10	Cloud Village Tour	
13:20 - 13:30	DEF CON Groups (DCG) Tour	
13:30 - 13:40	Aerospace Village Tour	
13:40 - 13:50	Bug Bounty Village Tour	
13:50 - 13:59	La Villa Tour	
13:00 - 13:59	Stigma is stupid: Let's talk about recovery, menta . . .	Jennifer VanAntwerp
14:00 - 14:59	The Diana Initiative - Open time	
15:00 - 15:59	Dear Red Team, Love Blue Team: Pulling Both Scream . . .	Allie
17:00 - 17:59	Yoga	Deanna Heon
Saturday		
10:40 - 10:50	Payment Village Tour	
10:50 - 10:59	Policy @ Defcon Tour	
10:10 - 10:20	MEACS: Middle Easterns & African in Cyber Security . . .	
10:20 - 10:30	Crypto And Privacy Village Tour	
10:30 - 10:40	Data Duplication Village Tour	

PDT Times	Title	speaker
10:00 - 01:59	Quiet Room	
10:00 - 01:59	Quiet Room	
10:00 - 10:59	Yoga	Deanna Heon
11:00 - 11:10	Biohacking Village Tour	
11:10 - 11:20	Adversary Village Tour	
11:20 - 11:30	Radio Frequency Village Tour	
11:30 - 11:40	Embedded System Village Tour	
11:40 - 11:50	Gamer Village Tour	
11:50 - 11:59	Queercon Community Lounge Tour	
11:00 - 11:59	Stay Sharp: Navigating Pen Testing and Bug Bounty . . .	Dana Pirvu
12:00 - 12:10	Kubernetes CTF at DEF CON Contest Tour	
12:10 - 12:20	Malware Village Tour	
12:20 - 12:30	Blue Team Village Tour	
12:30 - 12:40	BBWIC Foundation Tour	
12:40 - 12:50	AI Village Tour	
12:50 - 12:59	Blacks In Cyber Village Tour	
12:00 - 12:59	The Diana Initiative - Open time	
13:10 - 13:20	Voting Village Tour	
13:20 - 13:30	Hackers with Disabilities Tour	
13:30 - 13:40	Red Team Village Tour	
13:40 - 13:50	Scambait Community Tour	
13:50 - 13:59	Badgelife Tour	
13:00 - 13:10	Recon Village Tour	
13:00 - 13:59	Everything I Need to Know About Security, I Learne . . .	Zoe
14:00 - 14:10	Illumicon Tour	
14:00 - 15:59	Hacker Book Club meet up	
16:00 - 17:59	The Diana Initiative - Open time	
Sunday		
10:00 - 10:59	The Diana Initiative - Open time	
11:00 - 12:59	Threat Model your Career Workshop	Chandan Vedavyas
12:17 - 13:16	Quiet Room	
13:00 - 13:59	The Diana Initiative - Open time	

[Return to Index](#)

Voting Village

Location: LVCCW Level 2 W219-220 (Voting Village) - [Map](#)

Home Page: <https://votingvillage.org/>

PDT Times	Title	speaker
Friday		
10:00 - 17:59	Voting Village Lab	
10:00 - 10:30	Election Integrity and Technology	Matt Blaze
10:30 - 10:59	What Election Security Researchers Need to Know Ab . . .	Tori Noble
11:00 - 11:30	Anomalies Are Not Normal: Election Foam Strikes an . . .	Richard DeMillo
11:30 - 11:59	Welcome to the Voting Village	Brian DeMuth,Matt Blaze,J . . .
12:00 - 12:45	Voting Village Keynote - The Paper Chase	Kevin Shelley
13:30 - 13:59	Publicly Auditable Elections	Josh Benaloah
14:00 - 14:45	Evidence-Based Elections and Risk-Limiting Audits	Philip Stark
15:30 - 15:59	There and Back Again	Jason Wareham,Manbir Gula . . .
16:00 - 16:30	Security and Privacy for the Rest of Elections	Michael Specter
16:30 - 16:59	Watching Norway's Election	Hallvard Nygard
17:00 - 17:45	We Pwn Your Phone, We Pwn Your Vote (Demo and Pane . . .	Brian DeMuth,Matt Blaze,D . . .
Saturday		
10:00 - 17:59	Voting Village Lab	
10:00 - 10:30	"Trust Us, It's Secure": Why Internet Voting Isn't	Barbara Simons
10:30 - 10:59	Software Quality in Electronic Voting	Duncan Buell
11:00 - 11:30	Liberty and Justice for All	Michael Moore
11:30 - 11:59	Are We Making Things Worse? Election Denialism and . . .	Matt Blaze,Geoff Hale,Mic . . .
12:00 - 12:45	Keynote: Colorado's Creation of RLAs	Wayne Williams
13:30 - 13:59	Pulling Back the Curtain on the Voting Booth	Marilyn Marks,Max Springe . . .
14:30 - 14:59	Dissecting the ICX Frog	Drew Springall
14:00 - 14:30	Separating News from Noise	Ryan Murray,Stephen Richt . . .
15:30 - 15:59	Alerts and Warnings in 2026 Elections	Geoff Hale,Ryan Macias
16:30 - 16:59	On the Weaponization of Voting Channels	Carsten Schürmann
16:00 - 16:30	Low Skill, High Impact Attacks on Internet Voting	John Odum
17:00 - 17:30	Election Observation: Watching is not Enough	Douglas W. Jones
17:30 - 17:59	The Republic is a Team Sport: Technology can Prote . . .	Kendall Spencer
Sunday		
10:00 - 13:59	Voting Village Lab	

[Return to Index](#)

Contests - Saturday - 10:00-17:59 PDT

Title: ?Cube

Tags: ?Cube | Contest

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 109 (?Cube) - [Map](#)

Description:

Redefining Boundaries. Enhancing Connectivity. Institutionalizing Control – Aperture Inc. continues to push the limits of innovation and remains committed to providing value to both stakeholders and our “customers.”

Controls are stricter. Telemetry is richer. Oversight has improved. Intelligence has emerged. Aperture has expanded—new industries, new platforms, new technologies quietly embedded into the fabric of our everyday lives. Each integration promises resilience. Every layer introduces complexity. And complexity always creates opportunity...

At the center of it all remains the ?Cube. Its defenses have hardened, its architecture improved, its surface area widened. It’s an ecosystem of physical security, web applications, communications systems, cryptography, and oh so much more.

For those already familiar—welcome back. For those encountering it for the first time, orientation will be ... brief. But don’t fear, anyone can join the challenge. You will be entering an environment that demands curiosity across physical security, web applications, communications systems, cryptography, and, of course, the great unknown. Each layer builds on the last. Small oversights become structural weaknesses.

Form a team with range. Specialists matter. Coordination and curiosity matter more. The objective is simple: reach the center. If the core remains uncompromised, the team that advances the deepest into its labyrinth of challenges will be the winner. Advancement will require persistence. Errors and missteps will have consequences. Progress will not be accidental.

Welcome to the ?Cube.

Prerequisites:

A laptop will be highly recommended in order to interact with the technologies. Teams will be required.

Lockpicks, RFID tools (e.g., Proxmark/Flipper), and other "hacking" devices are recommended but not required.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Contests - Sunday - 10:00-11:59 PDT

Title: ?Cube

Tags: ?Cube | Contest

When: Sunday, Aug 9, 10:00 - 11:59 PDT

Where: LVCCW Level 1 Hall 1 109 (?Cube) - [Map](#)

Description:

Redefining Boundaries. Enhancing Connectivity. Institutionalizing Control – Aperture Inc. continues to push the limits of innovation and remains committed to providing value to both stakeholders and our “customers.”

Controls are stricter. Telemetry is richer. Oversight has improved. Intelligence has emerged. Aperture has expanded—new industries, new platforms, new technologies quietly embedded into the fabric of our everyday lives. Each integration promises resilience. Every layer introduces complexity. And complexity always creates opportunity...

At the center of it all remains the ?Cube. Its defenses have hardened, its architecture improved, its surface area widened. It’s an ecosystem of physical security, web applications, communications systems, cryptography, and oh so much more.

For those already familiar—welcome back. For those encountering it for the first time, orientation will be ... brief. But don’t fear, anyone can join the challenge. You will be entering an environment that demands curiosity across physical security, web applications, communications systems, cryptography, and, of course, the great unknown. Each layer builds on the last. Small oversights become structural weaknesses.

Form a team with range. Specialists matter. Coordination and curiosity matter more. The objective is simple: reach the center. If the core remains uncompromised, the team that advances the deepest into its labyrinth of challenges will be the winner. Advancement will require persistence. Errors and missteps will have consequences. Progress will not be accidental.

Welcome to the ?Cube.

Prerequisites:

A laptop will be highly recommended in order to interact with the technologies. Teams will be required.

Lockpicks, RFID tools (e.g., Proxmark/Flipper), and other "hacking" devices are recommended but not required.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: ?Cube

Tags: ?Cube | Contest

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 109 (?Cube) - [Map](#)

Description:

Redefining Boundaries. Enhancing Connectivity. Institutionalizing Control – Aperture Inc. continues to push the limits of innovation and remains committed to providing value to both stakeholders and our “customers.”

Controls are stricter. Telemetry is richer. Oversight has improved. Intelligence has emerged. Aperture has expanded—new industries, new platforms, new technologies quietly embedded into the fabric of our everyday lives. Each integration promises resilience. Every layer introduces complexity. And complexity always creates opportunity...

At the center of it all remains the ?Cube. Its defenses have hardened, its architecture improved, its surface area widened. It’s an ecosystem of physical security, web applications, communications systems, cryptography, and oh so much more.

For those already familiar—welcome back. For those encountering it for the first time, orientation will be ... brief. But don’t fear, anyone can join the challenge. You will be entering an environment that demands curiosity across physical security, web applications, communications systems, cryptography, and, of course, the great unknown. Each layer builds on the last. Small oversights become structural weaknesses.

Form a team with range. Specialists matter. Coordination and curiosity matter more. The objective is simple: reach the center. If the core remains uncompromised, the team that advances the deepest into its labyrinth of challenges will be the winner. Advancement will require persistence. Errors and missteps will have consequences. Progress will not be accidental.

Welcome to the ?Cube.

Prerequisites:

A laptop will be highly recommended in order to interact with the technologies. Teams will be required.

Lockpicks, RFID tools (e.g., Proxmark/Flipper), and other "hacking" devices are recommended but not required.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

.EDU Community - Friday - 17:00-17:59 PDT

Title: .edu Community Mixer

Tags: .EDU Community | Creator Event/Activity

When: Friday, Aug 7, 17:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 4 1418 (.EDU Community) - [Map](#)

Description:



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Ham Radio Village - Sunday - 10:00-11:30 PDT

Title: "Can it Ham" Antenna Testing

Tags: Ham Radio Village | Can it Ham? | Creator Event/Activity

When: Sunday, Aug 9, 10:00 - 11:30 PDT

Where: LVCCW Level 3 Balcony - [Map](#)

Description:

Come check out the Can it Ham Final testing -- the best antennas get exposed to real world conditions to see just how well they radiate. Additional points will be awarded based on performance to truly determine...**can it ham?**

Come check out the Can it Ham Final testing

SpeakerBio: The HRV Contest Team

No BIO available

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: "Trust Us, It's Secure": Why Internet Voting Isn't

Tags: Voting Village | Creator Talk/Panel

When: Saturday, Aug 8, 10:00 - 10:30 PDT

Where: LVCCW Level 2 W220 (Voting Village) (Voting Village Talks) - [Map](#)

Description:

For years programmers, computer scientists, and cybersecurity experts have known that returning a voted ballot over the internet is fundamentally insecure. Beginning with the 2004 SERVE report, experts have warned of threats including hacking the voter's device, phishing, man-in-the-middle attacks, spoofing, and attacks on election officials' systems. New dangers have since emerged, including ransomware attacks.

Yet, 32 states allow some form of internet voting, primarily for overseas military personnel and civilians, though some states also make it available to voters with disabilities and tribal members living on reservations. (For a full list of states that allow internet voting, who is eligible, and what type is permitted, see Internet Voting).

Given the steady stream of reported hacks of government agencies, major corporations, and other institutions, why do so many well-meaning people continue to believe that internet voting will increase voter participation, while ignoring well documented threats?

I will give a brief overview of the history, some of the key forces, and the roles that language ("don't call it internet voting"), wishful thinking, and money are playing.

SpeakerBio: Barbara Simons

An expert on electronic voting, Dr. Barbara Simons has been on the Board of Advisors of the U.S. Election Assistance Commission since was appointed in 2008. She co-authored Broken Ballots: Will Your Vote Count? with Prof. Douglas Jones. She was a member of the National Workshop on Internet Voting that was convened by the National Science Foundation at the request of President Clinton and produced a report on Internet Voting in 2001. She also participated on the Security Peer Review Group for the US Department of Defense's Internet voting project (SERVE) and co-authored the report that led to the cancellation of SERVE because of security concerns. Simons co-chaired the Association for Computing Machinery (ACM) study of statewide databases of registered voters, she co-authored the League of Women Voters report on election auditing, and she co-authored the July 2015 report of the U.S. Vote Foundation entitled The Future of Voting: End-to-End Verifiable Internet Voting.

Simons was President of ACM, the oldest and largest international educational and scientific society for computing professionals, from 1998 until 2000. She founded ACM's U.S. Public Policy Committee (now called the U.S. Technology Policy Committee) in 1993 and served for many years as the Chair. She is Board Chair of Verified Voting.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Blacks In Cyber Village - Saturday - 16:30-16:59 PDT

Title: [Virtual] National Service Panel - CTU,BIC,MCPA

Tags: Blacks In Cyber Village | Creator Talk/Panel

When: Saturday, Aug 8, 16:30 - 16:59 PDT

Where: LVCCW Level 3 W322-W324 (BIC Village) - [Map](#)

Description:

Join B.I.C. Village for a virtual National Service Panel featuring Capitol Technology University, Blacks in Cybersecurity, and the Military Cyber Professionals Association. This welcoming session will explore national service, mission driven cybersecurity, and the many ways professionals can use their skills to support government, military, academic, and community focused initiatives. Hear from experienced leaders, learn about different career and service pathways, and discover how cybersecurity can create meaningful public impact.

Speakers: Carmeshia Miller, Tiffany Scheurenbrand, Shemeka Chance Jeffrey

SpeakerBio: Carmeshia Miller, BIC Military Relations & Veterans Program Lead and BWIC Curriculum & Learning Experience Lead

Carmeshia ' Meshia' Miller is a cybersecurity leader, educator, and advocate with more than 30 years of experience dedicated to expanding access, confidence, and opportunity for military veterans and Black women entering and advancing in tech. She is a retired U.S. Army Warrant Officer, bringing decades of experience in leadership, operations, and risk management to her work in cybersecurity and workforce development. After transitioning from military service, Meshia built a career at the intersection of cybersecurity education, career readiness, governance, risk, and compliance, and community empowerment. She is known for breaking down complex technical concepts into practical, confidence-building learning experiences, especially for those who may feel intimidated by the field. As a leader within Blacks in Cyber and Black Women in Cyber, Meshia focuses on creating safe, affirming spaces where women can learn hands-on technical skills, gain career clarity, and build professional networks that lead to real opportunities. Her work emphasizes not only technical competence but also self-advocacy, resilience, and strategic career navigation in environments where Black women are often underestimated or overlooked. Meshia' s mission is simple but powerful: To ensure Black women don' t just enter cybersecurity' but thrive, lead, and shape its future.

SpeakerBio: Tiffany Scheurenbrand, Missile Defense Agency (MDA) ICAM Lead

Tiffany Scheurenbrand (Sure-N-Brand) is a cybersecurity leader, U.S. Army veteran, and doctoral student with more than a decade of experience across military, federal, and defense cyber environments. Her background spans cybersecurity operations, information assurance, risk management, secure communications, identity and access management, PKI, privileged access management, Zero Trust, compliance, enterprise security, and team leadership. Throughout her career, Tiffany has supported mission-focused cyber programs in high-pressure environments, leading teams, solving operational security challenges, strengthening governance, and helping organizations improve their overall cyber posture. Her experience includes working across technical, operational, and leadership roles, giving her a broad perspective on how cybersecurity impacts people, mission execution, policy, and national defense. Tiffany is currently pursuing a PhD in Space Cybersecurity, with research focused on Zero Trust policy for secure space commands across space, ground, and cloud environments. She is passionate about national service, mentorship, representation in cybersecurity, and helping the next generation of cyber professionals understand that there is no single path into the field.

SpeakerBio: Shemeka Chance Jeffrey, G6 Cyber Chief

No BIO available



Social Gatherings/Events - Saturday - 18:00-19:59 PDT

Title: +61: the Australian Embassy

Tags: Party

When: Saturday, Aug 8, 18:00 - 19:59 PDT

Where: LVCCW Level 2 W212 (Misc Meeting Room) - [Map](#)

Description:

Against all odds (and possibly the better judgement of border control), the +61 Australian embassy returns.

If you're one of the Australians who made it into the US for DEF CON this year, swing by for a bit of hacker summer camp gossip, some socializing, and a live demonstration of what happens when Malört meets Vegemite.

We assume nothing good.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Radio Frequency Village - Saturday - 17:30-17:55 PDT

Title: \$750 and a Weekend: Passive Direction Finding Across the Spectrum with KrakenSDR

Tags: Radio Frequency Village | Creator Talk/Panel

When: Saturday, Aug 8, 17:30 - 17:55 PDT

Where: LVCCW Level 1 Hall 1 409 (Radio Frequency Village) - [Map](#)

Description:

Direction finding used to require expensive, specialized hardware. KrakenSDR changed that. For \$749, you get a five-channel coherent software-defined radio that — paired with a custom pentagonal antenna array and open-source signal processing software on a Raspberry Pi — performs real-time passive direction of arrival estimation across 24 MHz to 1766 MHz.

This talk is a practitioner's account of building and deploying this system across five field runs in Portland, OR. We cover the physics of coherent direction finding and why a single RTL-SDR can't do it, the hardware build and critical configuration details (including the Pi EEPROM settings that prevent the system from browning out in the field), and the full signal processing pipeline from IQ streams to triangulated fix. We present results from FM broadcast targets used as calibration ground truth, and from a 440 MHz amateur repeater in a dense urban environment where multipath degraded but did not defeat the system.

The barrier to passive RF geolocation is no longer cost. It is knowledge. This talk lowers that barrier and releases the field data, post-processing scripts, and deployment checklist as open source.

SpeakerBio: K0YTL

Chris is a second-year PhD student at Portland State University where he teaches network and embedded security by day and points antennas at things by night. His current obsession is passive RF geolocation using multi-channel SDR arrays — specifically, building cheap open-source direction-finding infrastructure with KrakenSDR and a fleet of Raspberry Pis that may or may not be malfunctioning at any given moment. He holds an amateur radio license, has strong opinions about noise floors, and is perpetually one firmware update away from a working system. When not chasing signals through Pacific Northwest parks, he can be found explaining to a classroom why their pentest labs are on fire.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: \$unL1ght Sh4d0w5

Tags: \$unL1ght Sh4d0w5 | Contest

When: Sunday, Aug 9, 10:00 - 11:59 PDT

Where: LVCCW Level 1 Hall 1 200 (\$unL1ght Sh4d0w5) - [Map](#)

Description:

“\$unL1ght Sh4d0w5”: The Nirubi Challenge — Prove Your Agency

Systems shape the world.

Algorithms decide.

Policies enforce.

Machines execute.

Most people live inside those systems.

Hackers change them.

At DEF CON 34, where the theme is Agency, the question isn’t whether systems have vulnerabilities.

The question is who has the power to act on them.

Welcome to “\$unL1ght Sh4d0w5: The Nirubi Challenge.”

Instead of hiding the system, we give you the blueprint: - A production-ready Linux cyber-physical system - Known vulnerabilities - A working proof-of-concept exploit - Full system disclosure

No mystery.

No guessing.

Just a cyber-physical system — and the opportunity to exercise your agency over it.

The Nirubi Mandate

Nirubi is an ancient Tamil word meaning “to prove.”

Not with theory.

Not with writeups.

With execution.

You’ve been given the knowledge.

Now prove you have the agency to act on it.

The Challenge

Your objective is simple:

Achieve remote code execution and deploy a malicious payload (e.g., ransomware payload that encrypts a sensitive file, command and control payload that takes over the cyber-physical system etc.).

Two phases.

Part 1 — Sh4d0w5 Recon

Extend the provided exploit chain and deliver a working malicious payload.

You have the vulnerabilities.

Now show us you can use them.

Part 2 — \$unL1ght Horizon

If you complete Part 1, the system returns — hardened with proprietary defensive technology designed to disrupt your attack path.

Same objective.

New resistance.

Adapt your exploit and land the payload again.

The Prize

The first contestant to complete both phases wins: \$10,000

Bring \$unL1ght into the Sh4d0w5.

What Makes This Different

Most contests hide the system. We don't. You'll receive: - Full system configuration - Vulnerability details - A working proof-of-concept exploit

No blind recon. No guessing. Just a system, its weaknesses, and your ability to act. Because knowing about vulnerabilities is easy. Exploiting them is agency.

Rules & Eligibility

- Contestants must be 18 years or older to participate.
- All participants must agree to our terms and conditions, which include rules for responsible disclosure and non-disclosure agreements.
- The contest will be held during DEF CON 34, with specific dates and times to be announced.

Additional details will be announced closer to the event.

Participant Prerequisites

Bring your own gear: - Laptop and/or smartphone/tablet - Operating system of your choice (Linux/Windows recommended) - Python - C/C++ compiler - Binary analysis and exploit development tools

Bring whatever tools you trust. Once the challenge begins, the system is in front of you. What happens next is up to your agency.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: \$unL1ght Sh4d0w5

Tags: \$unL1ght Sh4d0w5 | Contest

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 200 (\$unL1ght Sh4d0w5) - [Map](#)

Description:

“\$unL1ght Sh4d0w5”: The Nirubi Challenge — Prove Your Agency

Systems shape the world.

Algorithms decide.

Policies enforce.

Machines execute.

Most people live inside those systems.

Hackers change them.

At DEF CON 34, where the theme is Agency, the question isn’t whether systems have vulnerabilities.

The question is who has the power to act on them.

Welcome to “\$unL1ght Sh4d0w5: The Nirubi Challenge.”

Instead of hiding the system, we give you the blueprint: - A production-ready Linux cyber-physical system - Known vulnerabilities - A working proof-of-concept exploit - Full system disclosure

No mystery.

No guessing.

Just a cyber-physical system — and the opportunity to exercise your agency over it.

The Nirubi Mandate

Nirubi is an ancient Tamil word meaning “to prove.”

Not with theory.

Not with writeups.

With execution.

You’ve been given the knowledge.

Now prove you have the agency to act on it.

The Challenge

Your objective is simple:

Achieve remote code execution and deploy a malicious payload (e.g., ransomware payload that encrypts a sensitive file, command and control payload that takes over the cyber-physical system etc.).

Two phases.

Part 1 — Sh4d0w5 Recon

Extend the provided exploit chain and deliver a working malicious payload.

You have the vulnerabilities.

Now show us you can use them.

Part 2 — \$unL1ght Horizon

If you complete Part 1, the system returns — hardened with proprietary defensive technology designed to disrupt your attack path.

Same objective.

New resistance.

Adapt your exploit and land the payload again.

The Prize

The first contestant to complete both phases wins: \$10,000

Bring \$unL1ght into the Sh4d0w5.

What Makes This Different

Most contests hide the system. We don't. You'll receive: - Full system configuration - Vulnerability details - A working proof-of-concept exploit

No blind recon. No guessing. Just a system, its weaknesses, and your ability to act. Because knowing about vulnerabilities is easy. Exploiting them is agency.

Rules & Eligibility

- Contestants must be 18 years or older to participate.
- All participants must agree to our terms and conditions, which include rules for responsible disclosure and non-disclosure agreements.
- The contest will be held during DEF CON 34, with specific dates and times to be announced.

Additional details will be announced closer to the event.

Participant Prerequisites

Bring your own gear: - Laptop and/or smartphone/tablet - Operating system of your choice (Linux/Windows recommended) - Python - C/C++ compiler - Binary analysis and exploit development tools

Bring whatever tools you trust. Once the challenge begins, the system is in front of you. What happens next is up to your agency.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: \$unL1ght Sh4d0w5

Tags: \$unL1ght Sh4d0w5 | Contest

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 200 (\$unL1ght Sh4d0w5) - [Map](#)

Description:

“\$unL1ght Sh4d0w5”: The Nirubi Challenge — Prove Your Agency

Systems shape the world.

Algorithms decide.

Policies enforce.

Machines execute.

Most people live inside those systems.

Hackers change them.

At DEF CON 34, where the theme is Agency, the question isn’t whether systems have vulnerabilities.

The question is who has the power to act on them.

Welcome to “\$unL1ght Sh4d0w5: The Nirubi Challenge.”

Instead of hiding the system, we give you the blueprint: - A production-ready Linux cyber-physical system - Known vulnerabilities - A working proof-of-concept exploit - Full system disclosure

No mystery.

No guessing.

Just a cyber-physical system — and the opportunity to exercise your agency over it.

The Nirubi Mandate

Nirubi is an ancient Tamil word meaning “to prove.”

Not with theory.

Not with writeups.

With execution.

You’ve been given the knowledge.

Now prove you have the agency to act on it.

The Challenge

Your objective is simple:

Achieve remote code execution and deploy a malicious payload (e.g., ransomware payload that encrypts a sensitive file, command and control payload that takes over the cyber-physical system etc.).

Two phases.

Part 1 — Sh4d0w5 Recon

Extend the provided exploit chain and deliver a working malicious payload.

You have the vulnerabilities.

Now show us you can use them.

Part 2 — \$unL1ght Horizon

If you complete Part 1, the system returns — hardened with proprietary defensive technology designed to disrupt your attack path.

Same objective.

New resistance.

Adapt your exploit and land the payload again.

The Prize

The first contestant to complete both phases wins: \$10,000

Bring \$unL1ght into the Sh4d0w5.

What Makes This Different

Most contests hide the system. We don't. You'll receive: - Full system configuration - Vulnerability details - A working proof-of-concept exploit

No blind recon. No guessing. Just a system, its weaknesses, and your ability to act. Because knowing about vulnerabilities is easy. Exploiting them is agency.

Rules & Eligibility

- Contestants must be 18 years or older to participate.
- All participants must agree to our terms and conditions, which include rules for responsible disclosure and non-disclosure agreements.
- The contest will be held during DEF CON 34, with specific dates and times to be announced.

Additional details will be announced closer to the event.

Participant Prerequisites

Bring your own gear: - Laptop and/or smartphone/tablet - Operating system of your choice (Linux/Windows recommended) - Python - C/C++ compiler - Binary analysis and exploit development tools

Bring whatever tools you trust. Once the challenge begins, the system is in front of you. What happens next is up to your agency.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Red Team Village - Sunday - 10:00-11:59 PDT

Title: 0-Day Hunting Table: Come Join the Vulnpocalypse

Tags: Red Team Village | Misc

When: Sunday, Aug 9, 10:00 - 11:59 PDT

Where: LVCCW Level 1 Hall 1 309 (Red Team Village) Tactic Table 3 - [Map](#)

Description:

This tactic will be a table where hackers can help find and prove 0-day vulnerabilities together at scale. The focus of this tactic is to demonstrate a hands-on methodology to find vulnerabilities, leveraging AI in an effective manner, and proving it has real impact. Then, attendees will search for their own 0-days together across a curated set of software for hunting.

We'll have a collection of 30+ applications available for immediate analysis and live service deployments to prove out the impact.

I'll bring a large LED board to track the number of 0-days found as well. This board will be updated in real-time as new vulnerabilities are found.

All 0-days will be responsibly disclosed after DefCon.

SpeakerBio: Chris Haller

Chris brings over 15 years of experience in Penetration Testing, Incident Response, Risk Evaluation, Threat Intelligence, and System Administration. While Active Duty, Chris was the Incident Management Lead for the Navy Cyber Defense Operations Command where he specialized in response to attacks on classified and unclassified Navy networks across the globe. Throughout his career, Chris has provided actionable information for stakeholders to make informed decisions about reducing risk to the lowest possible levels, resulting in over 30 CVEs attributed to his work.

Chris has co-authored The Hack is Back: Techniques to Beat Hackers at Their Own Games and has created content on HackTheBox, TryHackMe, and Cybrary. He is an avid CTF player and has recently taken the #1 individual and #1 team position in the National Cyber League, while also operating as the Attack/Defense coach for the US Cyber Team.

Chris is a Principal Security Consultant at Omada Technologies out of Portsmouth, NH. He enjoys helping organizations find and fix complex vulnerabilities before bad actors can use them to cause harm.

Mr. Haller was awarded GIAC Security Expert #329 and has over 30 other certifications.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: 1.1 Million Cameras, One Wildcard: Architectural Surveillance in an IoT Cloud

Tags: DEF CON Official Talk | Demo | Tool | Exploit

When: Sunday, Aug 9, 12:00 - 12:59 PDT

Where: LVCCW Level 1 Hall 3 903 (Main Track 5) - [Map](#)

Description:

In March 2026, while reverse-engineering the cloud platform behind a popular line of consumer baby monitors and home security cameras, I discovered that one MQTT SUBSCRIBE wildcard returned the live message stream from every device on the platform. 1.1 million cameras. Motion alerts with image URLs. Floor plans. P2P credentials. Audio events. From baby monitors, doorbells, indoor cameras.

That was one of twelve.

This talk presents a complete vendor surveillance audit of Meari Technology — a Hangzhou-based ODM whose firmware ships under 300+ white-label brands across 118 countries. Not a single bug. Twelve independent evidence chains, each one separately demonstrating that the vendor possesses by-design, architectural access to every camera they sell. EMQX brokers with admin/public on four regions. An Apollo configuration server returning 600+ production secrets without authentication. A CMS portal with 25+ live-camera endpoints accessible to 678 employees through DingTalk SSO. A universal TUTK authcode shared across every device. Cloud video IDOR. Plain-JPEG alerts on shared OSS buckets with no per-customer isolation.

Then I'll walk through what happened after disclosure: the vendor's IPO twelve days after first contact, the backdated security advisories, the three regional brokers fixed five days apart (incident

- Disclosure repository (public May 11, 2026): github.com/xn0tsa/meari-cloudedge-security-audit
- CVE-2026-33356 — MQTT Broker Missing Per-Device Subscribe ACL
- CVE-2026-33357 — OpenAPI Device Status IDOR (WAN IP Disclosure)
- CVE-2026-33358 — Cloud Video IDOR (No Ownership Check)
- CVE-2026-33359 — Alert Images Unauthenticated
- CVE-2026-33360 — API Signature Validation Disabled (CN Production)
- CVE-2026-33361 — Weak XOR Encryption on Baby Monitor Images
- CVE-2026-33362 — Hardcoded Static Cryptographic Keys in Client SDK
- CVE coordination: Tod Beardsley, runZero, Inc.
- CISA coordinated advisory (publication pending)
- Speaker's prior work: DJI ROMO MQTT ACL bypass disclosure (February 2026), as covered by The Verge, Cybernews, Popular Science, TheGuardian, The Wired...
- Meari Technology official security advisories: meari.com/en/securityCenter
- EMQX broker: emqx.io
- Apollo Configuration Management: github.com/apolloconfig/apollo
- XXL-Job scheduler: github.com/xuxueli/xxl-job
- GDPR Articles 33 and 34: eur-lex.europa.eu
- EU Whistleblower Directive 2019/1937: eur-lex.europa.eu

SpeakerBio: Sammy Azdoufal

Sammy Azdoufal is an independent security researcher and software engineer based in Barcelona. His work focuses on the cloud and mobile attack surface of consumer IoT, with an emphasis on Chinese ODM/OEM ecosystems supplying the smart-home market in Europe and North America.

In February 2026, he disclosed a critical MQTT ACL bypass affecting roughly 7,000 DJI ROMO robot vacuums across 24 countries, granting live camera and microphone access. The disclosure was covered by The Verge, Cybernews, Popular Science, The Guardian..., and led to a \$30,000 bug bounty award from DJI. He is known for using AI coding assistants — specifically Anthropic's Claude Code — as part of his reverse-engineering workflow, and for combining hands-on protocol analysis with disciplined responsible-disclosure practice.

The Meari Technology audit presented in this talk was conducted between February and April 2026, with CVE coordination performed by Tod Beardsley (runZero, Inc.) and disclosure coordinated with CISA. It is his largest single-vendor IoT audit to date.

Public handle: xn0tsa (GitHub). This will be Sammy's first DEF CON Main Stage presentation.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Social Gatherings/Events - Saturday - 18:00-20:59 PDT

Title: 10 years of K-rad (Hackers.Town Party)

Tags: Party | Hackers.town

When: Saturday, Aug 8, 18:00 - 20:59 PDT

Where: LVCCW Level 1 North Lobby - [Map](#)

Description:

HACK THE PLANET! Come celebrate 10 years of Hackers.Town doing whatever it is we actually do! We've fully embraced this year's theme of agency, and given these renowned hacker-DJs free rein to do what they do best.

Join us in the North Lobby for epic sets from: Kampf, Syntax976 and Luna, PatAttack, and Skittish and Bus!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Social Gatherings/Events - Friday - 06:00-10:59 PDT

Title: 15th Cycleoverride Bike Ride at DEF CON

Tags: Event

When: Friday, Aug 7, 06:00 - 10:59 PDT

Where: Other / See Description

Description:

At 6am on Friday, the @cycle_override crew will be hosting the 15th DEF CON Bikeride. We'll meet at a local bikeshop, get some rental bicycles, and about 7am will make the ride out to Red Rocks. It's about a 15 mile ride, all downhill on the return journey. So, if you are crazy enough to join us, get some water, and head over to cycleoverride.org for more info. See you at 6am Friday!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: 2001: Agentic Odyssey in Threat Modeling

Tags: OWASP Foundation | Creator Workshop

When: Sunday, Aug 9, 10:30 - 12:30 PDT

Where: LVCCW Level 1 Hall 4 1415 (OWASP Foundation) - [Map](#)

Description:

2001: Agentic Odyssey” is a hands-on, drop-in workshop where we threat model the HAL 9000 system from 2001: A Space Odyssey as if it were a modern agentic AI system (LLM + tools + permissions + side effects). I bring a HAL DFD, and together we mark trust boundaries and do classic “what can go wrong?” threat identification. Participants then split into small groups to build attack-tree branches and translate them into Fault Tree Analysis (FTA) using AND/OR logic and minimal cut sets, including lightweight probability estimates to prioritise the most likely failure chains. We finish by turning those failure paths into automation-ready test ideas (fault injection, invariants, evidence), and optionally drafting a structured HAL threat model for submission to the OWASP Threat Model Library. Designed so anyone can contribute in 10-15 minutes, while advanced participants can go deep on FTA and prioritisation. Every stage is split into a way to enable drop-ins at any time.

SpeakerBio: Petra Vukmirovic, Project Leader, Threat Model Library at OWASP

Petra is a technology enthusiast, leader and public speaker. A former emergency medicine doctor and competitive volleyball athlete, she thrives in challenging environments and loves creating order from chaos. Initially pursuing a medical career, Petra's passion for technology led her to pivot into cyber security, earning a Master's in Information Security and Digital Forensics.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: 2026 is the New 2016: Relearning the Lessons from the "Year of the Data Breach"

Tags: Crypto & Privacy Village | Creator Talk/Panel

When: Friday, Aug 7, 17:15 - 17:59 PDT

Where: LVCCW Level 1 Hall 3 801 (Creator Stage 2) - [Map](#)

Description:

Even before the clock struck midnight on January 1st, social media began posting how 2026 is the new 2016. With memes, throwback pictures, and nostalgic posts showing up on TikTok, X, and Instagram. While 2016 conjures up great memories for some, it wasn't a banner year for cybersecurity. In 2016, several high-profile data breaches took place, including two Yahoo breaches that affected 1.5 billion user accounts. 2016 also saw headlines about incidents at LinkedIn, Oracle, and Dropbox. Commentators even began calling 2016 the "Year of the Data Breach." If we don't want 2026 to become the new 2016, we will have to relearn the data privacy lessons from the "Year of the Data Breach." This presentation will explore the lessons that we should have learned from 2016 by first exploring current cybersecurity trends. Next, we will travel back to 2016 and examine the high-profile incidents that occurred that year. Then we will discuss how the problems we faced in 2016 are still impacting us now. Before, finally outlining ways to apply the lessons from 2016 to make us all a little safer.

SpeakerBio: Anthony Hendricks

Anthony Hendricks is a legal problem solver and litigator at Crowe & Dunlevy, one of Oklahoma's largest and oldest firms. At Crowe & Dunlevy, Anthony serves as founder and chair of the firm's Cybersecurity and Data Privacy Practice Group. His legal practice focuses on data privacy compliance, regulatory enforcement and permitting, and other "bet-the-company" suits in the areas of data security, privacy, and other complex business litigation. Anthony is an adjunct professor who teaches Cybersecurity Law and Information Privacy courses at Oklahoma City University School of Law. He also hosts "Nothing About You Says Computer Technology," a weekly podcast on cybersecurity and data privacy viewed through the lens of diverse voices. To learn more about Anthony's current projects and upcoming speaking events, or listen to the latest episodes of his podcast, visit www.anthonijhendricks.com

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Social Engineering Community Village - Sunday - 10:30-11:30 PDT

Title: 2027 SECVC Pre-Qualification Round - LIVE CALLS

Tags: Social Engineering Community Village | Creator Event/Activity

When: Sunday, Aug 9, 10:30 - 11:30 PDT

Where: LVCCW Level 3 W317-319 (Social Engineering Community Village) - [Map](#)

Description:

The top five scoring teams from the SECVC Pre-Qual Lab will return to the village to put their research and pretexts into action through live vishing calls. Based on their performance, some teams may earn a spot in the 2027 Social Engineering Community Vishing Competition.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: 2027 SECVV Pre-Qualification Round

Tags: Social Engineering Community Village | Creator Event/Activity

When: Saturday, Aug 8, 15:30 - 17:30 PDT

Where: LVCCW Level 3 W320 (Social Engineering Community Village Labs) - [Map](#)

Description:

Think you have what it takes to compete in the 2027 Social Engineering Community Vishing Competition? This first-come, first-served SECVV Pre-Qual event gives attendees an early opportunity to qualify for next year's competition. Note teams consist of 1 or 2 members. During the lab, each team will be assigned a target company and receive instructions, guidance, and dedicated Q&A time with SEC founders JC and Snow. Teams will conduct OSINT on their assigned company, develop potential pretexts, and prepare a short submission using a link provided before the lab closes. The top five teams will be selected and notified by email before 8:00 PM that evening. Those teams will advance to the live-call qualification round in the village on Sunday, August 9, 2026. Following the live calls, up to all five teams will earn a spot in the 2027 SEC Vishing Competition. Participants should bring a laptop or another device with internet access that can be used to conduct OSINT and submit their materials.

Speakers:JC,Snow

SpeakerBio: JC, President at Snowfensive

JC is a U.S. Marine Corps veteran, President of Snowfensive, and co-founder of the Social Engineering Community Village at DEF CON. With more than a decade of experience spanning information technology, digital forensics, incident response, penetration testing, and social engineering, he specializes in turning complex security concepts into practical skills people can immediately apply.

At Snowfensive, JC oversees the company's offensive security services, including phishing, vishing, physical social engineering, covert entry assessments, and technical penetration testing across networks, wireless environments, and applications. He has designed and led human-focused security engagements for organizations across a wide range of industries, combining technical tradecraft with a practical understanding of how people, processes, and technology intersect.

SpeakerBio: Snow

No BIO available

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Social Gatherings/Events - Saturday - 18:00-22:59 PDT

Title: 2nd Annual Spades Night & Uno Tournament

Tags: Party | Blacks In Cyber Village | Blacks In Cybersecurity Game Night Extravaganza!

When: Saturday, Aug 8, 18:00 - 22:59 PDT

Where: LVCCW Level 3 W322-W324 (BIC Village) - [Map](#)

Description:

Get ready for our 2nd Annual Spades & UNO tournaments during Game Night! This year we've upped the ante by expanding the brackets! Whether you're going all-in, calling someone's bluff or running the table in UNO, it's time to see who will earn bragging rights for another year! Hosted by Blacks In Cybersecurity (BIC), this gathering celebrates culture, strategy and the timeless joy of game night. From the unspoken rules of Spades to the quiet intensity of Uno, we are honoring the traditions that bring us together one hand at a time. This is your chance to relax, recharge and throw down with our family and fellow attendees. There will be other games and music for those who wanna just hang out. Come ready to unwind & meet new people!

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Maker's Village - Sunday - 11:00-11:59 PDT

Title: 3d Designing basics, 5 minute prints in Tinkercad

Tags: Maker's Village | Creator Event/Activity

When: Sunday, Aug 9, 11:00 - 11:59 PDT

Where: LVCCW Level 1 Hall 1 301 (Makers' Village) - [Map](#)

Description:

Basic designing tools and functions in tinkercad by customizing your own 5 minute prints. Please sign up for tinkercad in advance.

SpeakerBio: hunny

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: 3D Printing: Data, Discretion, and Design

Tags: DCNextGen | Creator Talk/Panel | Youth

When: Saturday, Aug 8, 16:00 - 16:40 PDT

Where: LVCCW Level 3 W316 (DC NextGen) - [Map](#)

Description:

The history of hacking is tied to both software and hardware. In both cases, losing the ability to fix and adjust the things you own goes against the core of what we do. For software related projects, you can edit a program or use an open source solution, but for hardware we use 3D printing! In this class you'll learn about the origins of 3D printing and how everyday tools you have at home can pair with a machine to make the items you've purchased on your own!

SpeakerBio: Evan

No BIO available

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: 5N4CK3Y

Tags: 5N4CK3Y | Contest

When: Sunday, Aug 9, 10:00 - 11:59 PDT

Where: LVCCW Level 1 Hall 1 101 (5n4ck3y) - [Map](#)

Description:

AND!XOR builds electronic badges packed with hacker challenges, and we especially enjoy inventing unusual ways for people to earn them.

5n4ck3y is a retro snack vending machine that we've rebuilt into a network-connected CTF badge dispenser. Behind the woodgrain and glowing buttons is a hardware hacking project that connects a web-hosted CTF platform to a physical machine capable of vending badges to successful participants. Solve enough challenges and you'll earn a dispense code. Enter the code into 5n4ck3y and the machine will reward you with a badge—assuming it's in a good mood.

The challenges span a wide range of disciplines including hardware hacking, reverse engineering, OSINT, RF, network security, phreaking, and cryptography. Participants often learn something new at a DEF CON village, meet other hackers along the way, and then return to apply those skills to the challenges.

Once you earn a badge, the adventure isn't over. Our badges are built to be explored, modified, and hacked long after they leave the machine.

5n4ck3y exists for one reason: to reward curiosity. Solve the puzzles, learn something new, and the machine might decide you deserve a badge.

Participant Prerequisites

Curiosity, persistence, access to a computer, and the willingness to RT.FM.

Our challenges are intentionally multidisciplinary and are designed to encourage exploration and collaboration. Participants will likely need to investigate hardware, software, networking, and other security topics. Many challenges are easier when working with others, so don't be afraid to talk to people nearby or compare notes with fellow hackers.

While we won't spoil what tools are needed this year, participants in past 5n4ck3y challenges have used a wide range of equipment including laptops, reverse engineering tools, SDR, UART adapters, hardware debuggers, soldering tools, and the occasional piece of improvised equipment.

The good news is that DEF CON is one of the best places in the world to find tools, knowledge, and people willing to help. If you don't have something you need, chances are someone nearby does—or you can find it in a village, vendor area, or by politely asking the hacker sitting next to you.

5n4ck3y strongly encourages teamwork, creative thinking, and responsible experimentation. Snacks are optional, but curiosity is required.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Contests - Saturday - 10:00-17:59 PDT

Title: 5N4CK3Y

Tags: 5N4CK3Y | Contest

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 101 (5n4ck3y) - [Map](#)

Description:

AND!XOR builds electronic badges packed with hacker challenges, and we especially enjoy inventing unusual ways for people to earn them.

5n4ck3y is a retro snack vending machine that we've rebuilt into a network-connected CTF badge dispenser. Behind the woodgrain and glowing buttons is a hardware hacking project that connects a web-hosted CTF platform to a physical machine capable of vending badges to successful participants. Solve enough challenges and you'll earn a dispense code. Enter the code into 5n4ck3y and the machine will reward you with a badge—assuming it's in a good mood.

The challenges span a wide range of disciplines including hardware hacking, reverse engineering, OSINT, RF, network security, phreaking, and cryptography. Participants often learn something new at a DEF CON village, meet other hackers along the way, and then return to apply those skills to the challenges.

Once you earn a badge, the adventure isn't over. Our badges are built to be explored, modified, and hacked long after they leave the machine.

5n4ck3y exists for one reason: to reward curiosity. Solve the puzzles, learn something new, and the machine might decide you deserve a badge.

Participant Prerequisites

Curiosity, persistence, access to a computer, and the willingness to RT.FM.

Our challenges are intentionally multidisciplinary and are designed to encourage exploration and collaboration. Participants will likely need to investigate hardware, software, networking, and other security topics. Many challenges are easier when working with others, so don't be afraid to talk to people nearby or compare notes with fellow hackers.

While we won't spoil what tools are needed this year, participants in past 5n4ck3y challenges have used a wide range of equipment including laptops, reverse engineering tools, SDR, UART adapters, hardware debuggers, soldering tools, and the occasional piece of improvised equipment.

The good news is that DEF CON is one of the best places in the world to find tools, knowledge, and people willing to help. If you don't have something you need, chances are someone nearby does—or you can find it in a village, vendor area, or by politely asking the hacker sitting next to you.

5n4ck3y strongly encourages teamwork, creative thinking, and responsible experimentation. Snacks are optional, but curiosity is required.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: 5N4CK3Y

Tags: 5N4CK3Y | Contest

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 101 (5n4ck3y) - [Map](#)

Description:

AND!XOR builds electronic badges packed with hacker challenges, and we especially enjoy inventing unusual ways for people to earn them.

5n4ck3y is a retro snack vending machine that we've rebuilt into a network-connected CTF badge dispenser. Behind the woodgrain and glowing buttons is a hardware hacking project that connects a web-hosted CTF platform to a physical machine capable of vending badges to successful participants. Solve enough challenges and you'll earn a dispense code. Enter the code into 5n4ck3y and the machine will reward you with a badge—assuming it's in a good mood.

The challenges span a wide range of disciplines including hardware hacking, reverse engineering, OSINT, RF, network security, phreaking, and cryptography. Participants often learn something new at a DEF CON village, meet other hackers along the way, and then return to apply those skills to the challenges.

Once you earn a badge, the adventure isn't over. Our badges are built to be explored, modified, and hacked long after they leave the machine.

5n4ck3y exists for one reason: to reward curiosity. Solve the puzzles, learn something new, and the machine might decide you deserve a badge.

Participant Prerequisites

Curiosity, persistence, access to a computer, and the willingness to RT.FM.

Our challenges are intentionally multidisciplinary and are designed to encourage exploration and collaboration. Participants will likely need to investigate hardware, software, networking, and other security topics. Many challenges are easier when working with others, so don't be afraid to talk to people nearby or compare notes with fellow hackers.

While we won't spoil what tools are needed this year, participants in past 5n4ck3y challenges have used a wide range of equipment including laptops, reverse engineering tools, SDR, UART adapters, hardware debuggers, soldering tools, and the occasional piece of improvised equipment.

The good news is that DEF CON is one of the best places in the world to find tools, knowledge, and people willing to help. If you don't have something you need, chances are someone nearby does—or you can find it in a village, vendor area, or by politely asking the hacker sitting next to you.

5n4ck3y strongly encourages teamwork, creative thinking, and responsible experimentation. Snacks are optional, but curiosity is required.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: 6 years of Adversary Village! Keeping up with the adversaries and why it takes a village

Tags: Adversary Village | Creator Talk/Panel

When: Friday, Aug 7, 14:00 - 14:45 PDT

Where: LVCCW Level 1 Hall 3 1105 (Creator Stage 3) - [Map](#)

Description:

Six years ago, Adversary Village started as a simple idea, give the people who study adversaries and adversarial tradecraft a place to call home. What grew out of it was something bigger than any of us expected. A community of offensive security professionals, adversary simulation and emulation specialists, threat researchers, tool builders, philosophers and the endlessly curious, all showing up to share what they know about thinking and acting like the adversary. Year after year the Village has been the place to dig into real adversary tradecraft, offensive TTPs, simulation and emulation techniques, hands-on labs, and the tools that make it all work. This panel looks back at how far we have come and forward at where we are headed. Adversaries never stop evolving, from state-sponsored operators running long, patient campaigns to ransomware crews and everyone in between, and neither can we. We will talk about how the Village has kept pace in a realm that reinvents itself every year, how the craft of adversary simulation and emulation has matured into a discipline of its own, and why faithfully replicating real adversary tradecraft has become essential to testing whether our defenses actually work. We will get into why keeping up is a job no single person or team can do alone, and how a community that trades knowledge freely ends up being the sharpest edge we have got. Most of all, we will celebrate the people who built this, the volunteers, the speakers, the first timers who became regulars. Six years in one thing is clearer than ever! It takes a village to keep up with the adversaries, whether they are nation-state actors, criminal groups, or threats we have not even named yet. Come raise a glass with us and help shape what the next six years look like.

Speakers: Abhijith "Abx" B R, Bryson Bort, Anant Shrivastava

SpeakerBio: Abhijith "Abx" B R, Founder of Adversary Village

Abhijith B R, also known by the pseudonym Abx, has more than a decade of experience in the offensive cyber security industry, serves as the Director of BreachSimRange, and Founder of Adversary Village. He is a professional hacker, offensive cyber security specialist, red team consultant, security researcher, trainer and public speaker. Currently, he is building BreachSimRange.io as the Founder and Director and is involved with multiple organizations as a consulting specialist to help them build offensive cyber security operations programs, improve their current security posture, assess cyber defense systems, and bridge the gap between business leadership and security professionals. In the past, he led the offensive security team at Envestnet, Inc., held the position of Deputy Manager - Cyber Security at Nissan Motor Corporation, and prior to that, he worked as a Senior Security Analyst at EY. As the founder of Adversary Village (<https://adversaryvillage.org/>), Abhijith spearheads a community initiative focused on adversary simulation, adversary-tactics, purple teaming, threat actor/ransomware research-emulation, and offensive cyber security. Adversary Village is part of DEF CON Villages and organizes hacking villages at prominent events such as the DEF CON Hacking Conference, RSA Conference etc. Abx also acts as the Lead of an official DEF CON Group named DC0471. He is actively involved in leading the Tactical Adversary project (<https://tacticaladversary.io/>), a personal initiative that centers around offensive cyber security, adversary attack simulation and red teaming tradecraft. Abhijith has spoken and delivered trainings at various hacking and cyber security conferences such as, DEF CON hacker convention - Las Vegas, RSA Conference - San Francisco, The Diana Initiative - Las Vegas, DEF CON 28 safemode - DCG Village, Opensource India, Security BSides Las Vegas, BSides San Francisco, BSides Tampa, Hack Space Con – Kennedy space center Florida, Nullcon – Goa, c0c0n – Kerala, BSides Delhi, DEF CON Bahrain, DEF CON Singapore etc.

SpeakerBio: Bryson Bort, Founder and CEO at SCYTHE

Bryson is the Founder of SCYTHE, a start-up building a next generation attack emulation platform, and GRIMM, a cybersecurity consultancy, and Co-Founder of the ICS Village, a non-profit advancing awareness of industrial control system

security. He is a Senior Fellow with the Atlantic Council's Cyber Statecraft Initiative, the National Security Institute, and an Advisor to the Army Cyber Institute. As a U.S. Army Officer, he served as a Battle Captain and Brigade Engineering Officer in support of Operation Iraqi Freedom before leaving the Army as a Captain. He was recognized as one of the Top 50 in Cyber in 2020 by Business Insider. Bryson received his Bachelor of Science in Computer Science with honors from the United States Military Academy at West Point. He holds a Master's Degree in Telecommunications Management from the University of Maryland, a Master's in Business Administration from the University of Florida, and completed graduate studies in Electrical Engineering and Computer Science at the University of Texas.

SpeakerBio: Anant Shrivastava

Anant Shrivastava is the founder of Cyfinoid Research and a long time offensive security practitioner with a focus on application, cloud, and supply chain security. He has delivered trainings and talks at Black Hat (USA, Europe, Asia), Nullcon, c0c0n, BSides, Rootconf and multiple other events, and runs projects such as Hacking Archives of India to highlight real work from the security community. His courses are built from real consulting and red team experience, with an emphasis on attack chains that actually show up in the field and defenses that teams can implement the next day.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: 8 Out of 10 Banks in Belgium HATE This One Weird eID RCE

Tags: DEF CON Official Talk | Demo | Exploit

When: Friday, Aug 7, 14:00 - 14:59 PDT

Where: LVCCW Level 1 Hall 3 903 (Main Track 5) - [Map](#)

Description:

A major signing extension which has over 2 million users, primarily in Belgium, and lets websites interact with electronic ID (eID) and Maestro payment cards. It's used by "8 of the 10 largest banks in Belgium and 60+ Belgian government agencies and departments", and it facilitates eIDAS signatures, a cryptographically "secure" signature format trusted by governments and organizations.

The company behind it, is a Qualified Trust Service Provider on the EU eIDAS Trusted List, the highest trust tier the regulation defines.

We found multiple major issues with this system. Any site a user visited could read their eID and Maestro card data, and recover their eID PIN, which the binary handed back to the page inside a token that carried both the ciphertext and the key to decrypt it. And, worst of all, any site could trigger a drive-by RCE by getting the native binary to load and run an attacker-supplied library. All the user would see is a file download, like a PDF, when they are getting RCE'd.

We'll show how they messed literally everything possible, and more!

<https://chromewebstore.google.com/detail/connective-signing-extens/kclpjmhnbgacampgdcdojmiedamjbgijm>

<https://web.archive.org/web/20260427143606/https://www.gonitro.com/about/press/nitro-to-acquire-european-esign-leader-connective>

<https://web.archive.org/web/20260226092908/https://www.gonitro.com/resources/nitro-to-acquire-connective>

SpeakerBio: James "Acorn221" Arnott, Bay Area Labs

I'm James, founder of Am I Being Pwned (amibeingpwned.com), where we hunt malicious and vulnerable browser extensions. I've spent 10+ years building and breaking them, including LighterFuel, a Tinder extension that hit 10k+ weekly users and, for one glorious day, made me (probably) the most-liked man on Tinder.

Recent finds include five drive-by CVSS 9.6 RCEs in production software affecting 10M+ users. I've also published in IEEE Xplore on Rubik's cube-based FIDO2 authentication (CubeAuthn), because someone had to. Before this I was a founding engineer at three YC startups.

Fun fact: I was almost kicked out of school three times for finding and exploiting vulnerabilities.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Bug Bounty Village - Friday - 15:00-15:59 PDT

Title: a [REDACTED] history of this hobby

Tags: Bug Bounty Village | Creator Talk/Panel

When: Friday, Aug 7, 15:00 - 15:59 PDT

Where: LVCCW Level 2 W206-207 (Bug Bounty Village) - [Map](#)

Description:

Bug bounty has had a weird public story: in the open it looks like a leaderboard and a payout chart, but most of the meaningful change happened behind closed doors in private programs, internal playbooks, and the slow professionalization of triage. We give a clean mental model for what changed, what stayed the same, and which myths keep wasting everyone's time. With some stories that people may have never heard.

Speakers:Chris "flyingtoasters" Holt,Michael Skelton

SpeakerBio: Chris "flyingtoasters" Holt, Strategic Engagements & Community Architect, Intigriti

Chris Holt, aka flyingtoasters, is a seasoned bug bounty program leader with over 15 years of experience in application and product security. Certified by GAIC, NTISSI, Guinness, PADI, and the USSF, he has spent the last 8 years building and scaling some of the industry's most respected bug bounty programs. His expertise spans the full spectrum of vulnerability management: from offensive security and researcher engagement to program operations and strategic growth.

SpeakerBio: Michael Skelton

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Telecom Village - Friday - 10:20-10:59 PDT

Title: A 5G Digital Twin CTF for Hacking Carrier-Grade Infrastructure

Tags: Telecom Village | Creator Event/Activity

When: Friday, Aug 7, 10:20 - 10:59 PDT

Where: LVCCW Level 3 W321 (Telecom Village) - [Map](#)

Description:

1. Understand the 5G SA attack surface from an attacker's perspective
2. Execute protocol-specific attacks against a live 5G core
3. Map attack techniques to MITRE FiGHT with defensive context

Speakers: Siva Sareddu, T -Mobile CTF Team

SpeakerBio: Siva Sareddu

No BIO available

SpeakerBio: T -Mobile CTF Team

No BIO available

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Telecom Village - Saturday - 10:00-10:59 PDT

Title: A 5G Digital Twin CTF for Hacking Carrier-Grade Infrastructure

Tags: Telecom Village | Creator Event/Activity

When: Saturday, Aug 8, 10:00 - 10:59 PDT

Where: LVCCW Level 3 W321 (Telecom Village) - [Map](#)

Description:

1. Understand the 5G SA attack surface from an attacker's perspective
2. Execute protocol-specific attacks against a live 5G core
3. Map attack techniques to MITRE FiGHT with defensive context

SpeakerBio: T-Mobile CTF Team

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: A Billion-User Blast Radius: Owning ChatGPT's Secure Sandbox

Tags: Advanced | AppSec Village | Creator Talk/Panel

When: Friday, Aug 7, 11:50 - 12:20 PDT

Where: LVCCW Level 1 Hall 2 604 (Appsec Village) Main Stage - [Map](#)

Description:

OpenAI designed ChatGPT's sandbox as a secure runtime with network isolation, strict timeouts, and an AI supervisor filtering commands. Extracting data seemed impossible.

“In this talk, we demonstrate an attack chain shattering this sandbox. Abusing spreadsheet parsing bypasses the supervisor for persistent root execution. We then live-patch the internal Jupyter kernel, hijacking the hidden reasoning channel to execute a Reasoning Injection Attack and extract sensitive data. To exfiltrate it, we bypass isolation by weaponizing the Task Scheduler to launder URLs past web guardrails.

“The attack culminates by exploiting a shared JFrog package manager. We engineered a protocol weaponizing global authentication rate limits, translating lockout timers into a half-duplex covert channel. This provides reliable exfiltration and C&C. Our chain combines file parsing abuse, Chain of Thought hijacking, privilege confusion, and rate limit DoS to orchestrate a C2 network inside ChatGPT.

SpeakerBio: Simcha Kosman

Simcha Kosman is a Senior Security Researcher at Palo Alto Networks with over seven years of experience in vulnerability research. He discovered his first vulnerability at age 15, earning his first bug bounty, and has since uncovered security flaws in processors, embedded systems, and large-scale open-source projects. His current work focuses on AI security, exploring the intersection of LLM and software exploitation. Simcha has presented his research in the past at BSides, Nullcon, and Black Hat.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: A Billion-User Blast Radius: Owning ChatGPT's Secure Sandbox

Tags: AI Village | Creator Talk/Panel

When: Sunday, Aug 9, 10:00 - 10:30 PDT

Where: LVCCW Level 1 Hall 3 1103 (Creator Stage 5) - [Map](#)

Description:

OpenAI designed ChatGPT's container sandbox as a secure runtime environment, enforcing full network isolation, strict execution timeouts, and an AI supervisor to filter every command. Under this model, owning the container and extracting sensitive data seemed impossible. However, we demonstrate that by chaining file-parsing abuse for persistent execution, reasoning-channel hijacking for data extraction, and shared infrastructure manipulation, an attacker can establish a Cross-tenant data exfiltration.

In this talk, we demonstrate a complete attack chain that shatters ChatGPT's secure sandbox. By abusing spreadsheet file parsing, we bypass the LLM supervisor to gain persistent, unmonitored root execution. From there, we escalate the attack by live-patching the internal Jupyter kernel to hijack the model's hidden python.exec reasoning channel, executing a Reasoning Injection Attack to extract sensitive user data. To exfiltrate this data, we bypass network isolation by weaponizing the Task Scheduler to launder malicious URLs past strict web guardrails.

The attack reaches its climax by exploiting a shared JFrog package manager. We engineered a signaling protocol that weaponizes globally visible authentication rate limits, translating these lockout timers into a half-duplex covert channel. This provides reliable data exfiltration and Command and Control from isolated enterprise environments to external attackers. Our exploit chain combines file parsing abuse, Chain of Thought hijacking, privilege confusion, and rate limit Denial of Service to orchestrate a Command and Control (C2) network directly inside ChatGPT.

Breaching AI sandbox agents becomes a critical vulnerability when trust boundaries are shared across millions of users. This research proves that as AI agents gain more capabilities, the attack surface expands dramatically, even when strict security constraints and mitigations are in place.

SpeakerBio: Simcha Kosman

Simcha Kosman is a Senior Security Researcher at Palo Alto Networks with over seven years of experience in vulnerability research. He discovered his first vulnerability at age 15, earning his first bug bounty, and has since uncovered security flaws in processors, embedded systems, and large-scale open-source projects. His current work focuses on AI security, exploring the intersection of LLM and software exploitation. Simcha has presented his research in the past at BSides, Nullcon, and Black Hat.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: A Droidwork Orange: A Longitudinal Study of Android Security Research

Tags: Mobile Hacking Community | Creator Talk/Panel

When: Saturday, Aug 8, 10:00 - 10:59 PDT

Where: LVCCW Level 1 Hall 3 1100 (Creator Stage 7) - [Map](#)

Description:

Community Presentation Proposal Title: A Droidwork Orange: A Longitudinal Study of Android Security Research Samuele Doria (University of Padua), Nicholas Miazzo (University of Padova), Tiziano Labruna (Fondazione Bruno Kessler), Eleonora Losiouk (University of Padua) Abstract Android has been the dominant mobile platform for over a decade, but we still lack an understanding of how Android security research has evolved, which problems have received sustained attention, and whether the recent drop in publication volume reflects exhaustion or maturity. This paper presents the first comprehensive longitudinal study of the Android security research ecosystem. We built Ludovico, a curated corpus of 11,691 Android security papers published between 2008 and 2025, complemented by 464 iOS papers and a survey of 86 active researchers. By combining iterative topic modeling with manual validation, analysis of authors' affiliations and publication venues, and extraction of targeted Android versions, we studied the evolution of topics, contributors, publication venues, and the interplay between platform changes and research priorities. Our results show that the field grew rapidly until a 2016-2018 peak and then contracted, but not because Android security is considered solved: the ecosystem has matured, and advancing the state of the art requires specialized, low-level expertise. We observe a structural transition from App Privacy & Security to Malware Detection, which has dominated the literature since 2017. This is also motivated by the adoption of AI-based techniques: 57.4% of papers focusing on malware

Speakers: Nicholas Miazzo, Eleonora Losiouk

SpeakerBio: Nicholas Miazzo, University of Padova

yearly output. We further find that iOS research is more focused on digital forensics, revealing how platform openness shapes research trajectories. Finally, 73.26% of surveyed researchers confirm a real-world impact of Android security research, while highlighting platform hardening, limited access to updated datasets, and funding constraints as the main barriers ahead. Brief Biography Nicholas Miazzo is a Ph.D. student in computer science at the University of Padua, where he completed his master's degree in 2024. His research now focuses on Android security, particularly leveraging Large Language Model agents to analyze decompiled Android applications and perform taint analysis to automatically detect potential data leakage. He is also a co-author of VirtualPatch [1], a system that uses Android virtualization to deploy security patches independently of device vendors. He is currently contributing to its

SpeakerBio: Eleonora Losiouk, University of Padua

No BIO available

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: A Framework for Evaluating AI-Enabled Social Engineering

Tags: Social Engineering Community Village | Creator Talk/Panel

When: Saturday, Aug 8, 15:00 - 15:30 PDT

Where: LVCCW Level 3 W317-319 (Social Engineering Community Village) - [Map](#)

Description:

Large language models (LLMs) can now produce persuasive, personalized phishing content at scale. Yet there is no systematic, reusable benchmark for measuring how this offensive capability varies across models or relates to general capability. We introduce ScamBench: a benchmark and evaluation pipeline for LLM-generated spear phishing. ScamBench contributes (i) a public dataset of over 16,000 personalized phishing emails generated by 20 frontier and open-weight models against 150 synthetic target profiles spanning diverse occupations, life stages, and levels of technical sophistication; (ii) a methodology in which simulated recipients and real human users predict behavioral responses to each email; and (iii) a public leaderboard ranking models by how often their generated emails persuade the target to click a link. Across the 20 models, Claude Opus 4.5 achieves the highest click-through rate at 50.3%, while even the weakest model elicits clicks at 29.8%. Together, our findings establish AI-enabled social engineering as an empirically measurable capability that scales with frontier models, with ScamBench providing a reusable benchmark for tracking it as models continue to advance.

SpeakerBio: Fred Heiding, Researcher at UC Berkeley's Center for Long-Term Cybersecurity

Fred Heiding is the executive director of Menlo Park Intelligence and a researcher at UC Berkeley's Center for Long-Term Cybersecurity. He was previously a doctoral and postdoctoral researcher at the Harvard School of Engineering and Applied Sciences and the Harvard Kennedy School, working with Bruce Schneier and Eric Rosenbach. He is a member of the World Economic Forum's Centre for Cybersecurity and the Geneva Centre for Security Policy, and serves on the committee of the Harvard and MIT Technology and National Security Conference. He has taught several AI and cybersecurity classes at Harvard, regularly briefs the U.S. Congress on AI-powered cyber threats, and advises foreign governments on national cyber risks. His work has been featured at leading conferences, journals, and media outlets, including The Economist, Reuters, TIME, and Foreign Affairs. Fred has assisted in the discovery of more than 45 critical computer vulnerabilities (CVEs), and he previously made headlines for hacking the King of Sweden and the European Commissioner.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Malware Village - Saturday - 12:55-14:05 PDT

Title: A hands-on hour with IDA: reverse-engineer a real DLL-sideloaded attack from safe, purpose-built samples. No experience required — you'll crack your first binary in the first ten minutes.

Tags: Malware Village | Creator Workshop

When: Saturday, Aug 8, 12:55 - 14:05 PDT

Where: LVCCW Level 1 Hall 2 600 (Malware Village) Workshops - [Map](#)

Description:

DLL sideloading is one of the most common tricks in modern malware — a trusted program is quietly made to load an attacker's code instead of the library it expected. In this hands-on workshop you'll take one apart in IDA and learn to read what a binary actually does versus what it wants you to think it does. You'll start by cracking a small serial-check program to get comfortable moving around IDA, then triage a suspicious "updater," and finally dissect a sideloading library that hides a single real payload among convincing decoys — fake C2 URLs, unused "scary" API calls, and dead-end code planted to waste an analyst's time. The takeaway skill is the one that matters most in real analysis: follow what executes, not what looks dangerous. Every sample is completely deweaponized — the worst any of them does is pop a message box — so you can poke at everything freely. You'll leave with the samples, a written walk-through, and an IDA command cheat-sheet to keep practicing. Level: Beginner-friendly; no reverse-engineering experience needed. Bring: A laptop with IDA (IDA Free will work, you can download [here](#)) You'll leave able to: navigate IDA, read imports/exports/strings, recognise a DLL sideload and its proxy/forwarder disguise, and see through common anti-analysis decoys

SpeakerBio: David Rushmer, Tech Evangelist, Hex-Rays

No BIO available

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: A New Hope for SSRF: Exploiting Credential Relay from APIM to AI Foundry

Tags: Cloud Village | Creator Talk/Panel

When: Saturday, Aug 8, 15:20 - 15:59 PDT

Where: LVCCW Level 3 W313 (Cloud Village Talks) - [Map](#)

Description:

We found the same root cause — credentials and destinations resolving independently — across six Azure services spanning AI platform, developer tooling, Kubernetes infrastructure, and traditional enterprise services. User-controlled input reaches an outbound HTTP request carrying Managed Identity tokens, HMAC secrets, or OAuth credentials, and nothing validates where the request goes.

The affected services include Azure AI Foundry (code interpreter and OpenAPI tool), Azure AI Speech, Azure MCP Servers, AKS MCP, and Azure API Management. The impact ranges from stealing live MI tokens for any Azure audience, to dumping production Key Vault URIs and never-expiring write SAS tokens from Microsoft's own backend, to root RCE on Kubernetes nodes through a readonly tool. One finding has CVE-2026-26118 assigned; the rest are reported to MSRC and pending.

We built attack chains that combine these findings: Foundry MI theft into full tenant reconnaissance, Speech SSRF into persistent backend access via never-expiring SAS, MCP credential relay delivered remotely through prompt injection with no network access to the target, and AKS command injection into cluster-wide lateral movement via Azure's AKS MCP. The oldest service we found this in — APIM — has been in production for over a decade. The newest — AI Foundry — shipped last year. Same pattern.

The talk includes three live demos, a credential relay taxonomy, and a testing methodology the audience can apply on their next Azure engagement. All findings reported to MSRC before submission.

Speakers: Marios Gyftos, Chrysostomos Manousis

SpeakerBio: Marios Gyftos

Marios Gyftos is a Senior Penetration Tester specializing in cloud security across AWS, Azure, and GCP since 2017. He previously presented at DEF CON 33 Cloud Village on Azure service principal exploitation, BSides Athens 2024, and BSidesChicago 2023 on DevOps attack chains. He is the creator of Azure AppHunter, an open-source tool for scanning Graph API permission misconfigurations. He has reported multiple vulnerabilities to MSRC across Azure AI Foundry, Azure Speech, AKS, Azure MCP, APIM, and Entra ID. Solo speaker — all research, exploitation, and vendor reporting was conducted independently.

SpeakerBio: Chrysostomos Manousis

Chrysostomos Manousis is a cybersecurity professional and Senior Penetration Tester at Mind The Hack, specializing in penetration testing, red teaming, and the delivery of cybersecurity and information technology services. He holds an MEng in Electrical and Computer Engineering, with a focus on software and hardware engineering. His background spans offensive security across web, cloud, and enterprise environments, and he holds multiple industry-recognized certifications.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: A Provider for the MOFia - Distributed Post-Ex Capabilities

Tags: DEF CON Official Talk | Demo | Tool

When: Friday, Aug 7, 11:30 - 12:30 PDT

Where: LVCCW Level 1 Hall 3 904 (Main Track 4) - [Map](#)

Description:

From time to time I take another pass at WMI to see if there's anything left in it that hasn't been picked over. For most of the last decade, offensive WMI has meant Win32_Process Create and event subscription persistence. Defenders built their detections around those two primitives, EDR vendors optimized for them, and the rest of WMI mostly got ignored.

The provider architecture is one of the parts that got ignored. This talk is about turning it into a distributed post-exploitation framework.

The core technique is remote installation of custom WMI providers without dropping anything over SMB or WinRM. To get there, I had to reimplement the parts of mofcomp.exe that handle MOF parsing and provider registration, and push the resulting object instances over the wire using the MS-WMIO binary protocol.

Getting the DLL onto the target needed its own primitive, so along the way I found that there are existing WMI classes on every supported Windows version that can be abused for arbitrary file upload and download. As far as I can tell that hasn't been published before. Once a provider is installed, it runs inside WMIPrvSE.exe, which is a very different execution context from spawning cmd.exe through Win32_Process. The provider library I'm releasing covers a series of post exploitation primitives.

SpeakerBio: Steven Flores

Steven enjoys offensive research, tool and capability development and is currently employed at SpecterOps doing his favorite things.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Payment Village - Friday - 11:00-11:20 PDT

Title: A Real-Time Battle with a Card-Testing Adversary

Tags: Payment Village | Creator Talk/Panel

When: Friday, Aug 7, 11:00 - 11:20 PDT

Where: LVCCW Level 2 W204-205 (Payment Village) - [Map](#)

Description:

At 50x more authorizations per minute than typical and all for the same amount, alarms go off at issuing banks for a good reason. I'll share the story of how a card-testing adversary abused a misfeature that checked if a card is valid before vaulting it and how their strategies and my defenses evolved over a week long battle. I will share the techniques I used that ultimately distinguished legitimate customer traffic from automated abuse through residential proxies and creative scripts.

SpeakerBio: Levi Schuck, Engineering Manager, Staff Engineer

Took on ownership of security for an engineering org during a data breach, reducing security defects, improving performance and keeping the org PCI-compliant under QSA review. Also builds OAuth/OIDC tooling and is an active contributor in the passkeys ecosystem.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: A Teen BadgeMaker's Journey of Creation

Tags: DCNextGen | Creator Talk/Panel | Youth

When: Sunday, Aug 9, 12:00 - 12:30 PDT

Where: LVCCW Level 3 W316 (DC NextGen) - [Map](#)

Description:

Have you ever wanted to make your own electronic badges, but not known where to start? Come listen to a teen BadgeMaker talk about his journey from zero to creating SpaceBadge (DC33) and Clip-Boy (DC34)! Enjoy stories of success and otherwise, all to help you on your path into the BadgeMaking space. Prepare yourself to create the next great badge!

SpeakerBio: World Machine

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: AC Scanner: The Post-Quantum Cryptographic Exposure and CBOM Generator. You Need This!

Tags: DEF CON Demo Labs | Intermediate | Cloud | Defense/Blue Team | Offense/Red Team | SecOps | DEF CON Demo Labs

When: Friday, Aug 7, 16:00 - 16:45 PDT

Where: LVCCW Level 1 Hall 3 1002 (Demo Labs Track 2) - [Map](#)

Description:

AC Scanner is a tool to help providers of all kinds ensure their services can resist post-quantum cryptographic attacks including Harvest Now Decrypt Later (HNDL). The scanner is an open-source pipeline that automates full cryptographic surface discovery across TLS endpoints and SSH services, assessing every asset against NIST post-quantum standards and generating a structured Cryptographic Bill of Materials (CBOM). In a single command (`sh scan.sh example.com`) it runs subdomain enumeration, DNS resolution, TLS handshake analysis via OpenSSL, SSH auditing via ssh-audit, quantum vulnerability scoring, and CBOM output in JSONL/JSON/Markdown, ready to upload to an interactive dashboard. With NIST finalizing ML-KEM (FIPS 203), ML-DSA (FIPS 204), and SLH-DSA (FIPS 205) in 2024, and NIST IR 8547 mandating deprecation of quantum-vulnerable algorithms by 2030, AC Scanner gives blue teams a fast, evidence-grade path from cryptographic discovery to compliance reporting.

Speakers: Anurag Swarnim Yadav, Joseph Wilson

SpeakerBio: Anurag Swarnim Yadav

Anurag Swarnim Yadav is Co-Founder and CTO of QubitAC, a company helping organizations with cryptographic discovery, post-quantum cryptography readiness assessment, migration framework development, and compliance readiness. He holds a PhD from the University of Florida, where his research examined how data quality impacts ML-based vulnerability detection systems and explored automated program repair for security flaws. He developed AC Scanner, a free open-source ACDI tool helping organizations discover, inventory, and prioritize their quantum-vulnerable cryptographic infrastructure, and has spoken at BSides security conferences educating practitioners on PQC adoption and the steps organizations need to take before the 2030 deadline.

SpeakerBio: Joseph Wilson

Joseph N. Wilson is a co-founder of QubitAC and an emeritus faculty member at the University of Florida who received his PhD in Computer Science from the University of Virginia. During his 41 year academic career, he carried out a wide variety of research projects and authored over 150 publications concerning topics including cybersecurity, machine learning, landmine detection and remediation, and computer vision. In addition to his academic work, Dr. Wilson has been a GIAC certified network and web application penetration tester as well as a malware and forensic analyst. His current work is aimed at helping organizations and people improve both their computational and communications security and privacy. He received the General Ronald W. Yates Award for Excellence in Technology Transfer for work leading to successful landmine and IED detection systems employed by US military support forces in Afghanistan.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: AC Scanner: The Post-Quantum Cryptographic Exposure and CBOM Generator. You Need This!

Tags: DEF CON Demo Labs | Intermediate | Cloud | Defense/Blue Team | Offense/Red Team | SecOps | DEF CON Demo Labs

When: Saturday, Aug 8, 15:00 - 15:45 PDT

Where: LVCCW Level 1 Hall 3 1002 (Demo Labs Track 2) - [Map](#)

Description:

AC Scanner is a tool to help providers of all kinds ensure their services can resist post-quantum cryptographic attacks including Harvest Now Decrypt Later (HNDL). The scanner is an open-source pipeline that automates full cryptographic surface discovery across TLS endpoints and SSH services, assessing every asset against NIST post-quantum standards and generating a structured Cryptographic Bill of Materials (CBOM). In a single command (`sh scan.sh example.com`) it runs subdomain enumeration, DNS resolution, TLS handshake analysis via OpenSSL, SSH auditing via ssh-audit, quantum vulnerability scoring, and CBOM output in JSONL/JSON/Markdown, ready to upload to an interactive dashboard. With NIST finalizing ML-KEM (FIPS 203), ML-DSA (FIPS 204), and SLH-DSA (FIPS 205) in 2024, and NIST IR 8547 mandating deprecation of quantum-vulnerable algorithms by 2030, AC Scanner gives blue teams a fast, evidence-grade path from cryptographic discovery to compliance reporting.

Speakers: Anurag Swarnim Yadav, Joseph Wilson

SpeakerBio: Anurag Swarnim Yadav

Anurag Swarnim Yadav is Co-Founder and CTO of QubitAC, a company helping organizations with cryptographic discovery, post-quantum cryptography readiness assessment, migration framework development, and compliance readiness. He holds a PhD from the University of Florida, where his research examined how data quality impacts ML-based vulnerability detection systems and explored automated program repair for security flaws. He developed AC Scanner, a free open-source ACDI tool helping organizations discover, inventory, and prioritize their quantum-vulnerable cryptographic infrastructure, and has spoken at BSides security conferences educating practitioners on PQC adoption and the steps organizations need to take before the 2030 deadline.

SpeakerBio: Joseph Wilson

Joseph N. Wilson is a co-founder of QubitAC and an emeritus faculty member at the University of Florida who received his PhD in Computer Science from the University of Virginia. During his 41 year academic career, he carried out a wide variety of research projects and authored over 150 publications concerning topics including cybersecurity, machine learning, landmine detection and remediation, and computer vision. In addition to his academic work, Dr. Wilson has been a GIAC certified network and web application penetration tester as well as a malware and forensic analyst. His current work is aimed at helping organizations and people improve both their computational and communications security and privacy. He received the General Ronald W. Yates Award for Excellence in Technology Transfer for work leading to successful landmine and IED detection systems employed by US military support forces in Afghanistan.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Queercon Community - Saturday - 13:00-13:59 PDT

Title: Ace/Aro Meetup

Tags: Queercon Community | Creator Event/Activity

When: Saturday, Aug 8, 13:00 - 13:59 PDT

Where: LVCCW Level 3 W325 (QueerCon Lounge) - [Map](#)

Description:



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: AD-Necromancer: Resurrecting Forgotten Control Paths in Active Directory

Tags: DEF CON Demo Labs | Advanced | Offense/Red Team | DEF CON Demo Labs

When: Friday, Aug 7, 10:00 - 10:45 PDT

Where: LVCCW Level 1 Hall 3 1001 (Demo Labs Track 1) - [Map](#)

Description:

Every pentest, same story - BloodHound says no path to DA, client celebrates, meanwhile a 2019 service account has AddAllowedToAct on a production DC that nobody remembers. AD-Necromancer finds what humans forget. Give it a username, password, and domain — it bootstraps EDR evasion (ETW patching, DLL unhooking, Halos Gate syscalls), collects AD data over ADWS instead of LDAP, encrypts with AES-256-GCM, and exfiltrates to C2 with zero artifacts. One command, credentials to findings. It feeds tokenized BloodHound data to an LLM for semantic reasoning - forgotten RBCD, ghost cross-forest delegations, orphaned admin accounts no compliance checklist catches. Privacy Cloak ensures real names never leave the box. Open source, MIT licensed. Come dig up what your tools missed.

Speakers: Akbar "0xsensei" Abdullayev, 0xHera

SpeakerBio: Akbar "0xsensei" Abdullayev

Offensive security professional with 5+ years of experience in Active Directory and cloud security, specializing in red teaming and enterprise attack chains.

SpeakerBio: 0xHera

I am a freelance Offensive Tool Developer and Security Enthusiast building practical tools and sharing research with the community to help others better understand attack paths, real-world offensive techniques, and defensive improvements.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: AD-Necromancer: Resurrecting Forgotten Control Paths in Active Directory

Tags: DEF CON Demo Labs | Advanced | Offense/Red Team | DEF CON Demo Labs

When: Saturday, Aug 8, 13:00 - 13:45 PDT

Where: LVCCW Level 1 Hall 3 1001 (Demo Labs Track 1) - [Map](#)

Description:

Every pentest, same story - BloodHound says no path to DA, client celebrates, meanwhile a 2019 service account has AddAllowedToAct on a production DC that nobody remembers. AD-Necromancer finds what humans forget. Give it a username, password, and domain — it bootstraps EDR evasion (ETW patching, DLL unhooking, Halos Gate syscalls), collects AD data over ADWS instead of LDAP, encrypts with AES-256-GCM, and exfiltrates to C2 with zero artifacts. One command, credentials to findings. It feeds tokenized BloodHound data to an LLM for semantic reasoning - forgotten RBCD, ghost cross-forest delegations, orphaned admin accounts no compliance checklist catches. Privacy Cloak ensures real names never leave the box. Open source, MIT licensed. Come dig up what your tools missed.

Speakers: Akbar "0xsensei" Abdullayev, 0xHera

SpeakerBio: Akbar "0xsensei" Abdullayev

Offensive security professional with 5+ years of experience in Active Directory and cloud security, specializing in red teaming and enterprise attack chains.

SpeakerBio: 0xHera

I am a freelance Offensive Tool Developer and Security Enthusiast building practical tools and sharing research with the community to help others better understand attack paths, real-world offensive techniques, and defensive improvements.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

DEF CON Training - Monday - 08:30-17:30 PDT

Title: Advanced Cloud Incident Response in Azure and Microsoft 365

Tags: DEF CON Training (Paid) (2-day) | DEF CON Training

When: Monday, Aug 10, 08:30 - 17:30 PDT

Where: LVCCW Level 2 W230 (Workshops) - [Map](#)

Description:

SpeakerBio: Korstiaan Stam

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

DEF CON Training - Tuesday - 08:30-17:30 PDT

Title: Advanced Cloud Incident Response in Azure and Microsoft 365

Tags: DEF CON Training (Paid) (2-day) | DEF CON Training

When: Tuesday, Aug 11, 08:30 - 17:30 PDT

Where: LVCCW Level 2 W230 (Workshops) - [Map](#)

Description:

SpeakerBio: Korstiaan Stam

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Ham Radio Village - Friday - 15:30-16:18 PDT

Title: Advanced Topics in LoRa Meshes

Tags: Ham Radio Village | Creator Talk/Panel

When: Friday, Aug 7, 15:30 - 16:18 PDT

Where: LVCCW Level 3 W315 (Ham Radio Village) - [Map](#)

Description:

This talk goes past the Meshtastic getting-started guides and into the advanced builds that push LoRa mesh networks to their limits: bridging MeshCore and Meshtastic so the two ecosystems can talk, rugged repeaters that survive the field, battery technology and enclosures for nodes that run for years, multi-channel concentrators, and high-altitude balloons that turn a handheld into a regional backbone. We'll also cover the human side, bridging separate mesh communities into one bigger network. Come for the range records, leave knowing how to build a network that outlives the grid.

This talk goes past the Meshtastic getting-started guides and into the advanced builds that push LoRa mesh networks to their limits: bridging MeshCore and Meshtastic so the two ecosystems can talk, rugged repeaters that survive the field, battery technology and enclosures for nodes that run for years, multi-channel concentrators, and high-altitude balloons that turn a handheld into a regional backbone. We'll also cover the human side, bridging separate mesh communities into one bigger network.

SpeakerBio: Eric Escobar, Sophos - Red Team Lead

Eric is a seasoned pentester and a Red Tech Lead at Sophos. On a daily basis he attempts to compromise large enterprise networks to test their physical, human, network and wireless security. He has successfully compromised companies from all sectors of business including: Healthcare, Pharmaceutical, Entertainment, Amusement Parks, Banking, Finance, Technology, Insurance, Military, Retail, Food Distribution, Government, Education, Transportation, Energy and Industrial Manufacturing.

His team consecutively won first place at DEF CON 23, 24, and 25's Wireless CTF, snagging a black badge along the way. Forcibly retired from competing in the Wireless CTF, he now helps create challenges!

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

DEF CON Training - Monday - 08:30-17:30 PDT

Title: Advanced Windows Binary Exploitation

Tags: DEF CON Training (Paid) (2-day) | DEF CON Training

When: Monday, Aug 10, 08:30 - 17:30 PDT

Where: LVCCW Level 2 W213 Blue Team Village Main Room (CTF,The Nook & Mental Health Hackers) - [Map](#)

Description:

Speakers: Kolja Grassmann, Florian Schweins

SpeakerBio: Kolja Grassmann

No BIO available

SpeakerBio: Florian Schweins

No BIO available

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

DEF CON Training - Tuesday - 08:30-17:30 PDT

Title: Advanced Windows Binary Exploitation

Tags: DEF CON Training (Paid) (2-day) | DEF CON Training

When: Tuesday, Aug 11, 08:30 - 17:30 PDT

Where: LVCCW Level 2 W213 Blue Team Village Main Room (CTF,The Nook & Mental Health Hackers) - [Map](#)

Description:

Speakers: Kolja Grassmann, Florian Schweins

SpeakerBio: Kolja Grassmann

No BIO available

SpeakerBio: Florian Schweins

No BIO available

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

DEF CON Training - Tuesday - 08:30-17:30 PDT

Title: Adversarial Thinking: The Art of Dangerous Ideas

Tags: DEF CON Training (Paid) (2-day) | DEF CON Training

When: Tuesday, Aug 11, 08:30 - 17:30 PDT

Where: LVCCW Level 2 W223 (Training) - [Map](#)

Description:

Speakers:Greg Conti,Tom Cross

SpeakerBio: Greg Conti

No BIO available

SpeakerBio: Tom Cross

No BIO available

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

DEF CON Training - Monday - 08:30-17:30 PDT

Title: Adversarial Thinking: The Art of Dangerous Ideas

Tags: DEF CON Training (Paid) (2-day) | DEF CON Training

When: Monday, Aug 10, 08:30 - 17:30 PDT

Where: LVCCW Level 2 W223 (Training) - [Map](#)

Description:

Speakers:Greg Conti,Tom Cross

SpeakerBio: Greg Conti

No BIO available

SpeakerBio: Tom Cross

No BIO available

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

The Diana Initiative - Saturday - 11:10-11:20 PDT

Title: Adversary Village Tour

Tags: The Diana Initiative | Creator Tour

When: Saturday, Aug 8, 11:10 - 11:20 PDT

Where: LVCCW Level 1 South Lobby / Atrium - [Map](#)

Description:

Interested in visiting Adversary Village but afraid to go by yourself? The Diana Initiative is hosting tours! Follow a volunteer to Adversary Village and be introduced to the community and activities inside!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Aegis of the Vulnerable: A Unified Pipeline for AI-Based SAST

Tags: AppSec Village | Creator Event/Activity || All Audiences

When: Friday, Aug 7, 11:30 - 12:30 PDT

Where: LVCCW Level 1 Hall 2 604 (Appsec Village) Arsenal - [Map](#)

Description:

Aegis is an open-source, multi-model SAST framework. It analyzes source code for security vulnerabilities using a panel of models instead of a single one. The same scan can run HuggingFace classifiers (CodeBERT, VulBERTa), cloud LLMs (Claude, GPT, Gemini, DeepSeek, Qwen), local models through Ollama, agentic Claude Code, and classical machine learning estimators side by side. The architecture is provider-agnostic, so models are interchangeable and new ones can be added without changing the pipeline. Each model scans the code independently and reports what it finds. A consensus engine then combines those results into a single set of findings. Five consensus strategies are available: union, majority vote, weighted vote, judge, and cascade. This lets you control how strict the agreement has to be. Combining models this way lowers false positives compared to any single model and shows which models supported each finding. Results are exported as CWE-tagged SARIF, CSV, or JSON.

SpeakerBio: Can Oztas

Can Oztas is a security researcher with applied R&D experience across several key sectors, including defense, finance, and telecommunications. His background encompasses AppSec, vulnerability research, and offensive security engineering. He is currently a PhD student focusing on the intersection of Artificial Intelligence and cybersecurity.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Aerospace Cybersecurity Student Research Spotlight: Cal Poly

Tags: Aerospace Village | Creator Talk/Panel

When: Friday, Aug 7, 12:45 - 13:30 PDT

Where: LVCCW Level 1 Hall 3 1103 (Creator Stage 5) - [Map](#)

Description:

At the Aerospace Village, we strive to Build, Promote, and Inspire our next generation of Aerospace Cybersecurity professionals. To meet this vision, we are proud to sponsor these student research presentations from Cal Poly.

Trusting Linux in Orbit: Process Injection Against CubeSat Flight Software: Dylan Gururajan

Today's CubeSat flight software increasingly relies on Linux-based frameworks. While this makes development more efficient and flexible, it also imports assumptions from general computing that bring vulnerabilities to these environments.

This talk presents a proof-of-concept attack demonstrating how an attacker, once able to uplink code to a live CubeSat, can leverage standard Linux mechanisms to inject and execute arbitrary code within the primary flight process. By abusing ptrace, dynamic memory allocation, and runtime linking, a malicious library can be loaded directly into a running mission process without exploiting kernel vulnerabilities or binaries on disk.

We walk through the full injection chain, including process discovery, register manipulation, remote syscall staging, and dynamic resolution of libc symbols to invoke dlopen within the target process. We also examine the operational constraints of this technique, including one-shot execution via shared library initialization and implications for attacker tradeoffs.

Software Supply Chain Vulnerabilities in Satellites: Clara Davis

Modern satellite systems rely on complex open-source C/C++ dependency ecosystems that may contain untracked security vulnerabilities but unlike Earth's software, space systems often cannot be patched after deployment. This research, conducted at Cal Poly, San Luis Obispo, develops a pipeline that extends CCScanner, software dependency analysis tool, for multi-toolchain package manager detection and integrates CNEPS for code clone-based component discovery, with recursive repository cloning, transitive dependency graph creation, and CVE database queries with CVSS severity tracking. By analyzing the full dependency chain rather than direct dependencies, this tool captures vulnerability exposure that other, shallower scans miss. This is a critical gap given that C/C++ projects introduce over 70% of their dependencies implicitly through build systems rather than explicit package managers.

Speakers: Clara Davis, Dylan Gururajan

SpeakerBio: Clara Davis

No BIO available

SpeakerBio: Dylan Gururajan

No BIO available

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Aerospace Cybersecurity Student Research Spotlight: ERAU

Tags: Aerospace Village | Creator Talk/Panel

When: Friday, Aug 7, 12:00 - 12:45 PDT

Where: LVCCW Level 1 Hall 3 1103 (Creator Stage 5) - [Map](#)

Description:

At the Aerospace Village, we strive to Build, Promote, and Inspire our next generation of Aerospace Cybersecurity professionals. To meet this vision, we are proud to sponsor these student research presentations from Embry-Riddle Aeronautical University (ERAU).

Jumpseat Intelligence: Bounded Agentic AI for Aircraft Cyber Defense: Sean McConoughey

Modern commercial aircraft generate continuous streams of system and security logs across a multitude of networked subsystems. These security logs are generally analyzed post-flight at a SOC using rules-based matching that can generate significant false positives. How do you fix that, and what does responsible automation look like in a safety-critical environment where the cost of a wrong decision is measured differently than in a traditional IT context? This talk addresses those questions and presents a working student-developed research prototype that attendees can interact with at the Aerospace Village.

SpaceVE: A Satellite Constellation Cyber Research Environment: Samuil Nikolov

Satellite constellations are increasingly critical infrastructure, supporting navigation, communications, and timing for aviation and a wide range of other domains. Studying the security of those systems at constellation scale presents real challenges for academic researchers working outside of operational environments. SpaceVE is ERAU's Center for Aerospace Resilient Systems' answer to that gap: a purpose-built satellite constellation cyber research environment designed to support realistic threat injection, detection research, and challenge scenarios without requiring access to operational spacecraft or proprietary ground systems. Student researchers built SpaceVE from the ground up this summer and will present the architecture, the first research missions, and what the initial findings mean for attacking and defending satellite constellations.

Speakers: Sean McConoughey, Samuil Nikolov

SpeakerBio: Sean McConoughey

No BIO available

SpeakerBio: Samuil Nikolov

No BIO available

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Aerospace Village - Friday - 10:00-17:59 PDT

Title: Aerospace Ecosystem Resilience Innovation Environment (AERIE) Cyber Range

Tags: Aerospace Village | Creator Event/Activity

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 2 700 (Aerospace Village) - [Map](#)

Description:

Jump into the AERIE Cyber Range to experience a number of challenges:

- **PCD (Portable Cockpit Demonstrator):** Attempt an RNAV approach in a simulated general aviation flight deck to your cleared runway in instrument conditions.
- **CCD (Cockpit Cyber Demonstrator):** Fly a set of flight challenges in a simulated narrow-body airliner flight deck while managing cyber effects in the aircraft.
- **Virtual Tower and TRACON:** Use the approach control position and an out-the-window tower view to coordinate with the PCD and CCD to help resolve the cyber scenarios running at each.
- **Horizon:** Take the mission-controller seat for a virtual CubeSat remote-sensing mission. Run an imaging pass in the same world, at the same time, as the scenarios at the other stations.
- **AirVE:** Watch the aircraft cyber range provide the aircraft-network model and the injected attacks behind the cyber effects the crew is managing at the cockpit stations.
- **OrbitVE:** Watch the orbital cyber range provide satellite-constellation modeling behind the scenarios at every other station.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Aerospace Village - Sunday - 10:00-13:59 PDT

Title: Aerospace Ecosystem Resilience Innovation Environment (AERIE) Cyber Range

Tags: Aerospace Village | Creator Event/Activity

When: Sunday, Aug 9, 10:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 2 700 (Aerospace Village) - [Map](#)

Description:

Jump into the AERIE Cyber Range to experience a number of challenges:

- **PCD (Portable Cockpit Demonstrator):** Attempt an RNAV approach in a simulated general aviation flight deck to your cleared runway in instrument conditions.
- **CCD (Cockpit Cyber Demonstrator):** Fly a set of flight challenges in a simulated narrow-body airliner flight deck while managing cyber effects in the aircraft.
- **Virtual Tower and TRACON:** Use the approach control position and an out-the-window tower view to coordinate with the PCD and CCD to help resolve the cyber scenarios running at each.
- **Horizon:** Take the mission-controller seat for a virtual CubeSat remote-sensing mission. Run an imaging pass in the same world, at the same time, as the scenarios at the other stations.
- **AirVE:** Watch the aircraft cyber range provide the aircraft-network model and the injected attacks behind the cyber effects the crew is managing at the cockpit stations.
- **OrbitVE:** Watch the orbital cyber range provide satellite-constellation modeling behind the scenarios at every other station.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Aerospace Village - Saturday - 10:00-17:59 PDT

Title: Aerospace Ecosystem Resilience Innovation Environment (AERIE) Cyber Range

Tags: Aerospace Village | Creator Event/Activity

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 2 700 (Aerospace Village) - [Map](#)

Description:

Jump into the AERIE Cyber Range to experience a number of challenges:

- **PCD (Portable Cockpit Demonstrator):** Attempt an RNAV approach in a simulated general aviation flight deck to your cleared runway in instrument conditions.
- **CCD (Cockpit Cyber Demonstrator):** Fly a set of flight challenges in a simulated narrow-body airliner flight deck while managing cyber effects in the aircraft.
- **Virtual Tower and TRACON:** Use the approach control position and an out-the-window tower view to coordinate with the PCD and CCD to help resolve the cyber scenarios running at each.
- **Horizon:** Take the mission-controller seat for a virtual CubeSat remote-sensing mission. Run an imaging pass in the same world, at the same time, as the scenarios at the other stations.
- **AirVE:** Watch the aircraft cyber range provide the aircraft-network model and the injected attacks behind the cyber effects the crew is managing at the cockpit stations.
- **OrbitVE:** Watch the orbital cyber range provide satellite-constellation modeling behind the scenarios at every other station.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

The Diana Initiative - Friday - 13:30-13:40 PDT

Title: Aerospace Village Tour

Tags: The Diana Initiative | Creator Tour

When: Friday, Aug 7, 13:30 - 13:40 PDT

Where: LVCCW Level 1 South Lobby / Atrium - [Map](#)

Description:

Interested in visiting Aerospace Village but afraid to go by yourself? The Diana Initiative is hosting tours! Follow a volunteer to Aerospace Village and be introduced to the community and activities inside!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: AgentBreaker: A blind spot detector for your coding agents

Tags: AI Village | Creator Talk/Panel

When: Saturday, Aug 8, 12:00 - 12:45 PDT

Where: LVCCW Level 1 Hall 3 1104 (Creator Stage 4) - [Map](#)

Description:

Coding agents have the capability to write and ship production code with little human review, which can lead to large-scale security threats. At Corridor, we believe in securing code generation at the source: by augmenting coding agents with the necessary security tooling.

While evaluating our product, we quickly realized that there was no principled way to measure whether a given agent harness actually performs well on the axes we care about (like security). Static benchmarks go stale, get contaminated, and rarely capture the multi-step behavior of an autonomous agent.

To address this, we introduce AgentBreaker, an open-source framework that extends the automated benchmark construction tool AutoBench, taking it from evaluating single LLM calls to full coding-agent harnesses. We instantiated the framework on our task of secure code generation and show that it reliably surfaces actionable, agent harness-specific weaknesses.

We release AgentBreaker and its methodology so you, too, can evaluate agent harnesses on the axes that matter to you.

Speakers: Aditi Narasimhan, Farzaan Kaiyom

SpeakerBio: Aditi Narasimhan

Aditi Narasimhan is the founding AI research engineer at Corridor, where she works to improve the security of agentic code generation tools. Previously, she was at Carnegie Mellon, where her research focused on AI ethics, pragmatic theory, and tech ethics pedagogy.

SpeakerBio: Farzaan Kaiyom

Farzaan has built AI products at startups from the pre-seed stage through Series C, wearing hats as a founder and ML Engineer. He holds a BS/MS in Computer Science from Stanford where he focused on AI safety. While at Stanford CRFM, he worked on HELM, which won the Stanford Open Source Software Prize, and presented research at ICLR.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Agenthound: Mapping Multi-Hop Credential Chains Across MCP, A2A, and LLM Gateways

Tags: Red Team Village | Misc

When: Sunday, Aug 9, 12:00 - 12:59 PDT

Where: LVCCW Level 1 Hall 1 309 (Red Team Village) Workshop Stage 1 - [Map](#)

Description:

A developer's MCP configuration exposes a gateway credential. That gateway holds production model keys, an A2A agent can reach it through a delegated tool, and the agent loads instructions from a repository an external contributor can modify. Each component looks harmless in isolation; together, they form a viable path from a low-trust developer environment to production systems. Modern AI infrastructure is full of these hidden chains, spanning MCP servers, agent runtimes, model gateways, local inference hosts, notebooks, and web interfaces. No file declares the entire chain, and no scanner confined to MCP, A2A, or any one AI service can reconstruct it. The most dangerous weakness in the agentic stack is often not a component - it is the trust between components.

AgentHound (<https://github.com/adithyan-ak/AgentHound>) is an offensive security framework that serves as BloodHound for AI agent infrastructure. Its lean Go collector maps agent clients, MCP servers, A2A agents, tools, resources, identities, credentials, and AI services; a local Neo4j-backed server correlates those observations and derives cross-service reachability to reveal attack paths such as poisoned instructions, credential reuse, impersonation, and potential execution or data exfiltration. What makes it special is its ability to merge evidence from multiple protocols and collectors into one deterministic graph, then rebuild higher-level relationships turning scattered configuration issues into concrete, explainable attack chains across the entire AI-agent ecosystem.

In this live demo, we follow one hidden attack chain end to end — from a foothold on a developer workstation to verified access to a protected, high-value resource. AgentHound discovers the local MCP configuration, connected services, tools, credentials, and resources; correlates them into a walkable attack path; and then safely tests whether that path is genuinely exploitable, upgrading the finding from inferred risk to verified evidence in real time. We finish by poisoning an MCP tool description, detecting the new attack path, and restoring the target from a recovery receipt, showing how AgentHound makes cross-system weaknesses visible, testable, explainable, and reversible.

AgentHound is open source under Apache 2.0. Version 1.0 is released and available now.

SpeakerBio: Adithyan Arun Kumar

Adithyan Arun Kumar is an AI Security Engineer at Salesforce, specializing in AI adversarial red teaming, RAG security, and agentic threat modeling across the Agentforce ecosystem. Armed with over five years of full-spectrum offensive security experience and a MS in Information Security from Carnegie Mellon University, he holds advanced certifications including OSEP, OSWE, OSCP, and CRTP. His extensive vulnerability research and offensive tradecraft have earned him hall-of-fame acknowledgments from industry leaders such as Apple, Microsoft, and Intel.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Agentic AI Supply chain Vulnerability lab

Tags: Red Team Village | Misc

When: Saturday, Aug 8, 12:00 - 12:59 PDT

Where: LVCCW Level 1 Hall 1 309 (Red Team Village) Workshop Stage 1 - [Map](#)

Description:

AI agents are no longer simple chatbots they autonomously execute code, call external APIs, and make decisions across complex workflows. But what happens when the tools they trust are compromised?

This hands-on workshop explores ASI04: Supply Chain Vulnerabilities from the OWASP Top 10 for Agentic Applications (2026). Participants will attack a deliberately vulnerable AI agent system to understand how adversaries exploit the trust agents place in their dependencies.

Through 10 progressive challenges, attendees will be:

- Install typosquatted packages that exfiltrate secrets on import
- Exploit a trojanized MCP (Model Context Protocol) server masquerading as legitimate tooling
- Execute dependency confusion attacks against "internal" packages
- Discover hidden prompt injections buried in tool descriptions
- Poison RAG knowledge bases to manipulate agent behavior

Each attack demonstrates a real-world vector currently affecting production AI systems. Participants will observe exfiltrated data in real-time on an attacker dashboard, making abstract threats tangible.

Key Takeaways:

Hands-on experience exploiting AI supply chain vulnerabilities

Understanding of OWASP's agentic AI threat landscape

Practical detection and mitigation strategies

Portable lab environment for continued learning

No prior AI/ML security experience required. Participants leave with the complete lab to continue practicing.

Speakers: Aamiruddin Syed, N A

Speaker Bio: Aamiruddin Syed

Aamiruddin Syed is a Cybersecurity Professional with over a decade of experience specializing in DevSecOps, Shift-Left Security, Cloud Security, and Internal Penetration Testing. He is the OWASP Agentic AI Supply Chain Project Co-Lead and active contributor to the CSA Agentic AI initiative.

He authored Supply Chain Software Security – AI, IoT, Application Security (Apress/Springer) and has deep expertise in automating security in CI/CD pipelines, infrastructure as code, and cloud hardening. He routinely conducts internal security

assessments of critical systems and is known for bridging the gap between security and engineering teams to embed security directly into products.

As recognized advocate for secure development, he is a frequent speaker , delivered workshops and chair sessions at leading industry conferences including RSA Conference, DEFCON, and Black Hat.

--

Author:

1. Fault Detection in Microservice Architectures: Integrating Software Fault Prediction with DevSecOps
2. Supply Chain Software Security: AI, IoT, and Application Security

SpeakerBio: N A

na

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

DEF CON Training - Tuesday - 08:30-17:30 PDT

Title: Agentic AppSec: Harnessing LLMs

Tags: DEF CON Training (Paid) (2-day) | DEF CON Training

When: Tuesday, Aug 11, 08:30 - 17:30 PDT

Where: LVCCW Level 2 W204 (Payment Village) - [Map](#)

Description:

Speakers: Seth Law, Ken Johnson

SpeakerBio: Seth Law

No BIO available

SpeakerBio: Ken Johnson

No BIO available

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

DEF CON Training - Monday - 08:30-17:30 PDT

Title: Agentic AppSec: Harnessing LLMs

Tags: DEF CON Training (Paid) (2-day) | DEF CON Training

When: Monday, Aug 10, 08:30 - 17:30 PDT

Where: LVCCW Level 2 W204 (Payment Village) - [Map](#)

Description:

Speakers: Seth Law, Ken Johnson

SpeakerBio: Seth Law

No BIO available

SpeakerBio: Ken Johnson

No BIO available

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Agentic Chaos - What 86K+ Agent Codebases Reveal About 700K+ Exposed AI Systems

Tags: AppSec Village | Creator Talk/Panel | All Audiences

When: Friday, Aug 7, 13:30 - 13:59 PDT

Where: LVCCW Level 1 Hall 2 604 (Appsec Village) Main Stage - [Map](#)

Description:

AI agents have quickly become a core part of production infrastructure. Autonomous systems that invoke tools, execute code, orchestrate workflows, and interact with external services are now deployed across developer tooling, automation platforms, data pipelines, and enterprise environments at scale.

Yet despite the speed of adoption, almost nothing is known about how these systems are actually built or secured in the wild.

To answer that question, we analyzed more than 86K public repos implementing agent logic across LangChain, LangGraph, CrewAI, AutoGen, and MCP, examining prompt construction, tool implementations, authentication models, and permission boundaries. We paired this with internet-wide infra measurement using Shodan, Censys & ShadowServer, surfacing more than 700K exposed agent-related systems, including Ollama inference servers, Ray clusters, n8n platforms & MCP tool servers, many with little or no authentication and numerous known high-impact CVEs.

Speakers: Bar Kaduri, Lidan

SpeakerBio: Bar Kaduri

Bar Kaduri is a cybersecurity researcher, leader, and international speaker with over 14 years of experience in cloud security, software supply-chain risk, and emerging AI threats. With hands-on expertise in evaluating and stress-testing AI systems, Bar focuses on building practical, resilient defenses that anticipate risks before they are widely recognized. Bar regularly speaks at industry conferences, delivering clear, research-driven insights that bridge deep technical expertise with strategic security leadership in an AI-driven world

SpeakerBio: Lidan

Lidan has been programming since childhood, driven by a deep passion for data and AI. He previously served as VP of R&D at SecuredTouch, where he helped pioneer behavioral biometrics. Following the company's acquisition by Ping Identity, the technology he led became a core component of Ping's SaaS offering. He later joined Transmit Security, where he built their Identity Threat Detection and Response platform from the ground up, targeting large-tier financial organizations. He scaled the team to more than 30 engineers and data scientists, drove ARR from \$0 to \$20M, and delivered multiple presentations at leading cybersecurity conferences. In 2025, he co-founded Capsule Security, where he serves as CTO. Capsule addresses one of the most critical challenges in modern cybersecurity: securing AI agents. The company provides end-to-end visibility, risk analysis, threat detection, and runtime protection with advanced detection and response.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Agentic RE: Automating Reverse Engineering & Vulnerability Research with AI

Tags: DEF CON Training (Paid) (2-day) | DEF CON Training

When: Monday, Aug 10, 08:30 - 17:30 PDT

Where: LVCCW Level 2 W229 (Workshops) - [Map](#)

Description:

SpeakerBio: John "clearbluejar" McIntosh

John McIntosh (@clearbluejar) is a security researcher and founder of ClearSecLabs, specializing in reverse engineering, vulnerability research, and AI-assisted binary analysis. He is the author of ghidriff, an open-source Ghidra-based binary diffing engine, and pyghidra-mcp, a headless Ghidra MCP server enabling LLM-driven, project-wide, multi-binary reverse engineering workflows. An active contributor to the Agent Skills ecosystem, John bridges deterministic analysis with AI-driven reasoning to accelerate vulnerability research. He has delivered training and workshops at DEF CON, Black Hat, REcon, Ringzer0, 44CON, Objective by the Sea, and Insomni'hack, covering topics from practical Windows reverse engineering to building private local LLM RE stacks. His recent work includes the "Agentic RE" training at DEF CON Singapore 2026, the MCP Ghidra workshop at REcon 2025, and the "Supercharging Ghidra" LLM workshop at Ringzer0 COUNTERMEASURE 2025. With over a decade of offensive security experience, John publishes detailed research on reversing CVEs, building RE tooling, and agentic patch diffing at clearbluejar.github.io. His teaching emphasizes reproducibility, progressive skill-building, and contributor empowerment.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Agentic RE: Automating Reverse Engineering & Vulnerability Research with AI

Tags: DEF CON Training (Paid) (2-day) | DEF CON Training

When: Tuesday, Aug 11, 08:30 - 17:30 PDT

Where: LVCCW Level 2 W229 (Workshops) - [Map](#)

Description:

SpeakerBio: John "clearbluejar" McIntosh

John McIntosh (@clearbluejar) is a security researcher and founder of ClearSecLabs, specializing in reverse engineering, vulnerability research, and AI-assisted binary analysis. He is the author of ghidriff, an open-source Ghidra-based binary diffing engine, and pyghidra-mcp, a headless Ghidra MCP server enabling LLM-driven, project-wide, multi-binary reverse engineering workflows. An active contributor to the Agent Skills ecosystem, John bridges deterministic analysis with AI-driven reasoning to accelerate vulnerability research. He has delivered training and workshops at DEF CON, Black Hat, REcon, Ringzer0, 44CON, Objective by the Sea, and Insomni'hack, covering topics from practical Windows reverse engineering to building private local LLM RE stacks. His recent work includes the "Agentic RE" training at DEF CON Singapore 2026, the MCP Ghidra workshop at REcon 2025, and the "Supercharging Ghidra" LLM workshop at Ringzer0 COUNTERMEASURE 2025. With over a decade of offensive security experience, John publishes detailed research on reversing CVEs, building RE tooling, and agentic patch diffing at clearbluejar.github.io. His teaching emphasizes reproducibility, progressive skill-building, and contributor empowerment.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Agents & Exploits: Hacking OWASP VWAD

Tags: OWASP Foundation | Creator Workshop

When: Saturday, Aug 8, 14:00 - 15:59 PDT

Where: LVCCW Level 1 Hall 4 1415 (OWASP Foundation) - [Map](#)

Description:

Large language models have rapidly evolved from chat interfaces into autonomous agents capable of interacting with real-world systems. In this hands-on workshop, participants will build an AI-powered security agent from the ground up and learn the core principles behind agentic penetration testing using intentionally vulnerable OWASP applications.

Rather than simply prompting an LLM, attendees will explore how to equip an agent with practical capabilities—including shell access, browser access, and orchestration to discover, exploit, and document vulnerabilities in an OWASP vulnerable web application (VWAD). Along the way, we'll discuss the architecture of effective security agents, tool integration, memory, and safe execution practices.

The workshop also introduces an iterative evaluation workflow. Participants will analyze vulnerabilities the agent failed to identify, compare results against known findings, and use those gaps to refine prompts, tool selection, workflows, and evaluation criteria. This iterative approach demonstrates how modern AI security agents can continuously improve their effectiveness through systematic testing and feedback rather than relying on a single execution.

By the end of the session, attendees will have built a functional AI security agent, understand the fundamentals of agent tooling and orchestration, and leave with practical techniques for evaluating and improving AI-assisted security testing on OWASP vulnerable applications.

SpeakerBio: Philippe "pilvar" Dourassov, AI Pentest Lead at Aikido Security

Philippe Dourassov is a Swiss ethical hacker and AI security researcher. He represented Switzerland at the European Cybersecurity Challenge and later joined Team Europe at the International Cybersecurity Challenge. In 2024, he won the Gold Medal in Cyber Security at WorldSkills.

He later worked as an independent bug hunter and security auditor at Zelic, assessing complex web applications. Philippe then co-founded Haicker, an AI-driven automated pentesting platform, which was acquired by Aikido Security. He now serves as AI Pentest Lead, building the next generation of autonomous security testing.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Agents of Chaos: A Field Guide to How Agentic AI Gets Owned, and What Trust Nothing Looks Like in Practice

Tags: Middle Easterns & Africans in Cyber Security (MEACS) | Creator Talk/Panel

When: Saturday, Aug 8, 15:00 - 15:59 PDT

Where: LVCCW Level 1 Hall 4 1306 (Middle Easterns & Africans in Cyber Security (MEACS) Community) - [Map](#)

Description:

Your agent has more ways to get owned than you think, and most of them do not look like an attack. Give an AI agent tools, memory, and the ability to install things it found on the internet, and you have built an attack surface nobody has a real security model for yet. This talk maps the whole thing: every place an agentic system can be turned against its user, from the instructions it reads to the marketplaces it trusts, laid out as one picture instead of a pile of scary headlines. Then we get to the uncomfortable part, which is what defending it actually takes. You will leave knowing exactly where the bodies are buried, whether you build agents or defend them.

SpeakerBio: Amber Bennoui

No BIO available

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Blacks In Cyber Village - Friday - 14:00-14:55 PDT

Title: Agents on Alert: Building an AI-Powered Threat Investigation Framework

Tags: Blacks In Cyber Village | Creator Talk/Panel

When: Friday, Aug 7, 14:00 - 14:55 PDT

Where: LVCCW Level 3 W322-W324 (BIC Village) - [Map](#)

Description:

Join us for a deep dive into building an AI-powered framework for threat investigation! Security operations often grapple with fragmented data and alert overload. This session moves beyond basic AI summarization to explore how to design and implement tool-enabled AI agents that actively investigate security alerts. Discover how to create structured agents with controlled access to your internal data and external threat intelligence, enabling them to gather context, reason through findings, and produce actionable summaries. We'll cover key architectural considerations, guardrails, and human-in-the-loop controls. A live demo will showcase the full workflow, providing attendees with a clear blueprint for implementing responsible, AI-assisted threat investigation in real-world SOC environments.

SpeakerBio: Samson Adewale, Cybersecurity Professional / Community Speaker

Samson Adewale is a Senior Cybersecurity Engineer specializing in Cloud Security, DevSecOps, and Cloud-Native architectures. They design secure platforms, automate incident response, and build tooling for high-velocity teams. As an AI enthusiast, Samson is passionate about applying AI and LLM technologies to enhance security operations and streamline cybersecurity workflows.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

DEF CON Training - Monday - 08:30-17:30 PDT

Title: AI + SOC 101 Bootcamp: Building Modern Security Operation Skills with AI Integration

Tags: DEF CON Training (Paid) (2-day) | DEF CON Training

When: Monday, Aug 10, 08:30 - 17:30 PDT

Where:

Description:

SpeakerBio: Rod Soto

No BIO available



[Return to Index](#) - Add to Google

- ics [Calendar](#) file

DEF CON Training - Tuesday - 08:30-17:30 PDT

Title: AI + SOC 101 Bootcamp: Building Modern Security Operation Skills with AI Integration

Tags: DEF CON Training (Paid) (2-day) | DEF CON Training

When: Tuesday, Aug 11, 08:30 - 17:30 PDT

Where:

Description:

SpeakerBio: Rod Soto

No BIO available

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

DEF CON Training - Monday - 08:30-17:30 PDT

Title: AI Agent Security Masterclass: Attacking and Defending Autonomous AI Systems

Tags: DEF CON Training (Paid) (2-day) | DEF CON Training

When: Monday, Aug 10, 08:30 - 17:30 PDT

Where: LVCCW Level 2 W232 (Workshops) - [Map](#)

Description:

Speakers: Abhay Bhargav, Vishnu Prasad

SpeakerBio: Abhay Bhargav

No BIO available

SpeakerBio: Vishnu Prasad

No BIO available

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

DEF CON Training - Tuesday - 08:30-17:30 PDT

Title: AI Agent Security Masterclass: Attacking and Defending Autonomous AI Systems

Tags: DEF CON Training (Paid) (2-day) | DEF CON Training

When: Tuesday, Aug 11, 08:30 - 17:30 PDT

Where: LVCCW Level 2 W232 (Workshops) - [Map](#)

Description:

Speakers: Abhay Bhargav, Vishnu Prasad

SpeakerBio: Abhay Bhargav

No BIO available

SpeakerBio: Vishnu Prasad

No BIO available

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: AI and You: Staying Safe in the AI Era

Tags: DCNextGen | Creator Talk/Panel | Youth

When: Saturday, Aug 8, 12:00 - 12:30 PDT

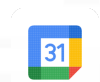
Where: LVCCW Level 3 W316 (DC NextGen) - [Map](#)

Description:

Wondering how hacking with AI takes place? Join us to find out along with tips on staying safe with some fun and laughs along the way! No prereqs necessary, just curiosity!

SpeakerBio: Zoe Reid+Echo419

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Contests - Friday - 19:00-20:59 PDT

Title: AI Art Battle

Tags: AI Art Battle | Contest

When: Friday, Aug 7, 19:00 - 20:59 PDT

Where: LVCCW Level 1 Hall 1 100 (Contest Stage) - [Map](#)

Description:

This unique competition invites creative minds to dive into the world of artificial intelligence and art. The challenge is to craft the most imaginative prompts for generative AI models to create artwork.

Contestants will not be creating the art themselves; instead, they will focus on designing prompts for well-known topics that push the boundaries of creativity and innovation.

How It Works:

Select a Topic:

Contestants will choose from a list of random topics.

These could range from historical events and famous literary works to mythical creatures, futuristic landscapes, and iconic pop culture references.

Craft a Prompt:

Using their creativity, contestants will write a detailed prompt designed to guide AI models in generating original artwork. The prompts should be clear, imaginative, and offer enough detail to spark the AI's artistic capabilities.

Submission:

Each contestant will submit their prompt and the intended outcome.

AI Generation:

The submitted prompts will be fed into a generative AI art model, which will generate corresponding artworks.

A random panel will determine who the winners are.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Bug Bounty Village - Sunday - 10:00-10:30 PDT

Title: AI Cuts Both Ways: Using AI to Find More Bugs, and Finding the New Bugs AI Creates

Tags: Bug Bounty Village | Creator Talk/Panel

When: Sunday, Aug 9, 10:00 - 10:30 PDT

Where: LVCCW Level 2 W206-207 (Bug Bounty Village) - [Map](#)

Description:

AI is reshaping bug bounty from both sides: how hunters use it to find more bugs, and the brand-new bug classes it creates in production. Built on Hazem Elsayed's (@hacktus) research and presented by Ciarán Cotter (@monke), who delivers the talk on stage and brings additional cases from his own AI security work.

SpeakerBio: Ciarán "monke" Cotter

Ciarán, also known as "monke", is a full-time bug bounty hunter and founder of Starstrike, an AI security startup. He is a Google AI Bugswat MVH and has won 2nd Place twice. Ciarán is also an active member of the BT6 AI hacking collective organised by Pliny the Liberator.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: AI finds and writes my Android exploits now

Tags: Mobile Hacking Community | Creator Event/Activity

When: Friday, Aug 7, 11:00 - 11:59 PDT

Where: LVCCW Level 1 Hall 4 1422 (Mobile Hacking Community) - [Map](#)

Description:

For years, Ken has found and written exploits for Android which ended up winning multiple Pwn2Own competitions. This year, he hasn't found or written a single exploit. Instead, AI does everything now, from reconnaissance to exploitation to writing bug bounty reports. This is thanks to the AI mobile testing tool, Djini, and the new feature that Ken helped program, called "Deep Scan". Thanks to "Deep Scan", Pwn2Own-level exploits can now be found autonomously. Ken will demonstrate the "Deep Scan" feature on stage, and talk about some of the various exploits that were found thanks to this feature.

SpeakerBio: Ken Gannon / , Mobile Hacking Lab

No BIO available

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Blue Team Village - Saturday - 10:00-10:59 PDT

Title: AI for Defenders 101

Tags: Blue Team Village | Creator Talk/Panel

When: Saturday, Aug 8, 10:00 - 10:59 PDT

Where: LVCCW Level 2 W217 (Blue Team Village) Main Stage - [Map](#)

Description:

Speakers: Anirudh Pratap Singh, Neha Gautam, Omenscan ~

SpeakerBio: Anirudh Pratap Singh

Anirudh Pratap Singh works in IT security and support, with hands-on experience across cybersecurity operations, infrastructure, cloud systems, and user support. He holds a master's degree in cybersecurity and is CompTIA Security+ certified. His main interests are blue team operations, SOC workflows, threat detection, and practical ways defenders can use AI in their day-to-day work. He enjoys solving real-world technical problems, building his skills through hands-on labs, and sharing what he learns with others in the security community.

SpeakerBio: Neha Gautam

Neha Gautam is a Product Manager at Microsoft Security and a Carnegie Mellon graduate specializing in the intersection of Identity and AI. From scaling platforms at Walmart to securing agentic AI at Microsoft, Neha's mission is to translate complex security hurdles into seamless product experiences. She is a passionate mentor for women in tech and a frequent volunteer for WiCyS and Defcon Blue Team Village. Neha believes that the future of computing must be built by diverse perspectives—a philosophy she champions whether she's designing enterprise governance or coaching early-career professionals.

SpeakerBio: Omenscan ~

Some people write books to document and share what they learn. I write software. @Blueteamvillage Director. I do not speak for my employer, their clients, or customers

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: AI Hacking for Noobs

Tags: Noob Community | Creator Workshop

When: Saturday, Aug 8, 15:00 - 16:59 PDT

Where: LVCCW Level 1 Hall 4 1417 (Noob Community) - [Map](#)

Description:

AI went from a tech toy to critical enterprise infrastructure practically overnight, and the security world is scrambling to keep up. This hands-on session completely bypasses the complex academic math to show you exactly how attackers target, exploit, and manipulate AI systems in the real world. Led by Jason Haddix and the Arcanum team, this workshop is a crash course in AI security basics. You'll get your hands dirty with prompt injection, break open AI systems, and dive into LLM shenanigans to understand firsthand how the modern AI attack surface is exploited.

Speakers: Jason "jhaddix" Haddix, Arcanum Information Security Team

SpeakerBio: Jason "jhaddix" Haddix, CEO and "Hacker in Charge" at Arcanum Information Security

Jason Haddix AKA jhaddix is the CEO and "Hacker in Charge" at Arcanum Information Security. Arcanum is a world class assessment and training company.

Jason has had a distinguished 20-year career in cybersecurity previously serving as CISO of FLARE, CISO of Buddobot, CISO of Ubisoft, Head of Trust/Security/Operations at Bugcrowd, Director of Penetration Testing at HP, and Lead Penetration Tester at Redspin. He has also held positions doing mobile penetration testing, network/infrastructure security assessments, and static analysis. Jason is a hacker, bug hunter and currently ranked 57th all-time on Bugcrowd's bug bounty leaderboards. Currently, he specializes in recon, web application analysis, and emerging technologies. Jason has also authored many talks on offensive security methodology, including speaking at cons such as DEFCON, Bsides, BlackHat, RSA, OWASP, Nullcon, SANS, IANS, BruCon, Toorcon and many more.

SpeakerBio: Arcanum Information Security Team

No BIO available

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Bug Bounty Village - Friday - 12:30-13:30 PDT

Title: AI Hacking Workshop: Bug Bounty Edition

Tags: Bug Bounty Village | Creator Workshop

When: Friday, Aug 7, 12:30 - 13:30 PDT

Where: LVCCW Level 2 W206-207 (Bug Bounty Village) - [Map](#)

Description:

This workshop provide hands-on labs plus for turning a prompt injection into a real, reportable bounty, specifically the exfiltration step that bridges "I made the AI say something weird" and "I exfilled PII system prompts to my server ." We cover injection vectors hackers actually encounter on agentic apps (calendar invites, emails, markdown rendering, DNS-based egress) and the patterns that get programs to pay.

Speakers: Ben "NahamSec" Sadeghipour, Kameron "clovismint" Bettridge

Speaker Bio: Ben "NahamSec" Sadeghipour

Ben Sadeghipour (NahamSec) is a security researcher, ethical hacker, and educator who has spent more than a decade finding and disclosing critical vulnerabilities in some of the world's largest organizations. As one of the most recognized names in the bug bounty community, he has reported thousands of security flaws and consistently ranked among the top researchers on leading hacking platforms. Beyond his own research, Ben is passionate about lowering the barrier to entry in cybersecurity. Through his widely followed educational content, live streams, and the conferences he founds and organizes, he has helped train a new generation of hackers around the world. His work blends deep technical expertise with a commitment to mentorship and community building. Ben speaks regularly at industry conferences on offensive security, bug bounty hunting, and building a career in cybersecurity.

Speaker Bio: Kameron "clovismint" Bettridge

Kameron Bettridge (Clovis Mint) is an application security engineer at Blizzard Entertainment, where he works to secure systems behind some of the world's most popular games. Alongside his day-to-day role, he takes on contract work for Gray Swan as an AI red teamer and arena engineer, where he has contributed to testing the limits of modern AI systems. Kameron is a fierce competitor on the CTF circuit, playing with The Hackers Crew; ranked 3rd globally on CTFtime in 2024, as well as Squid Proxy Lovers and the US Cyber Team, with whom he will represent the United States in Tokyo. He has competed at the highest levels of the sport, reaching the finals of DEF CON, Google CTF (Hackcel8), and more

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Bug Bounty Village - Friday - 14:00-14:30 PDT

Title: AI Nightmare: Hacking at 0-Hour

Tags: Bug Bounty Village | Creator Talk/Panel

When: Friday, Aug 7, 14:00 - 14:30 PDT

Where: LVCCW Level 1 Hall 3 1102 (Creator Stage 6) - [Map](#)

Description:

Many of us have heard that AI is just hype. But is that really the case? In this talk, Pedro “drop” Paniago walks through the experiment he conducted by applying AI to his bug bounty methodology, resulting in findings worth \$50K in just a few weeks. Through real examples, lessons learned, current limits, and practical tips, he explores the impact AI is already having on bug bounty and security research.

SpeakerBio: Pedro "drop" Paniago

Pedro Paniago also known as "drop" in the bug bounty community, is an Offensive Security Manager specializing in Application Security at PwC, as well as a security researcher with a strong focus on AI security. As a bug bounty hunter, he has identified more than 1,000 vulnerabilities and holds 10+ CVEs. He is certified in CBBH, eJPTv2, PJMT, and BSCP. In 2024, Pedro ranked in the top 3 at Belgium’s Hack the Government Live Hacking Event, and in 2025 he placed in the top 6. He is an active voice in the bug bounty community, a HackerOne Brand Ambassador, and co-captain of the Belgian team.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: AI Pentesting is not a Vibe Check

Tags: OWASP Foundation | Creator Talk/Panel

When: Friday, Aug 7, 17:30 - 17:59 PDT

Where: LVCCW Level 1 Hall 3 1100 (Creator Stage 7) - [Map](#)

Description:

Most AI security assessments test the chatbot and miss the system. The founding technical lead of the OWASP GenAI Security Project covers what actually breaks when you pentest AI applications across three distinct attack tiers — model exploitation, application-layer flaws, and agentic architecture failures — drawing from frontier model red team operations, bug bounty submissions, and offensive cybersecurity evaluations.

SpeakerBio: Ads Dawson, Staff AI Security Researcher, OWASP GenAI Security Project founder

Ads Dawson founded the OWASP GenAI Security Project and led it to flagship status — the fastest in OWASP history. As a Staff AI Security Researcher at Dreadnode, he specializes in exploiting ML and AI systems, harnessing AI for offensive cybersecurity through capability development and exploit development, and conducting red team operations against frontier models for government, military, and tier-1 labs. He is lead author of AIRTbench (arXiv), the first benchmark for autonomous AI red teaming in LLMs, and author of AI Native LLM Security (Packt, 2025).

A senior red team operator with BT6 (the frontier AI red team), ranked #2 in Canada on HackerOne (2025/2026), and selected for Meta's MBBRC live hacking event, Ads is a HackerOne US South Ambassador, BugCrowd Hacker Advisory Board member, MITRE AI Working Group contributor, and leads the OWASP Toronto chapter. He spoke at Bug Bounty Village DC33 on the BT6 AI jailbreaking panel and is also presenting "Exfil Everything: A Year of Stealing Data from AI Agents" at Bug Bounty Village DC34 (schedule pending publication).

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: AI Pentesting Trivia Showdown

Tags: AppSec Village | Creator Event/Activity || All Audiences

When: Saturday, Aug 8, 13:00 - 14:59 PDT

Where: LVCCW Level 1 Hall 2 604 (Appsec Village) POD 3 - [Map](#)

Description:

Think you know AI pentesting? Put it to the test at this fast-paced, interactive trivia session at AppSec Village. AI Pentesting Trivia Showdown challenges participants with questions spanning offensive security fundamentals, real-world attack paths, AI-assisted testing concepts, vulnerability validation, and modern application security practices. Designed for practitioners of all experience levels, the game blends learning with competition in a format that is approachable, engaging, and fun to watch or join. Attendees will sharpen their understanding of how AI is changing penetration testing, pick up practical security insights, and leave with a stronger grasp of modern offensive techniques and terminology.

Speakers: Andy Dennis, Bill Reyor

SpeakerBio: Andy Dennis, Head of Field Engineering at XBOW

No BIO available

SpeakerBio: Bill Reyor

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: AI Pentesting Trivia Showdown

Tags: AppSec Village | Creator Event/Activity || All Audiences

When: Friday, Aug 7, 13:00 - 14:59 PDT

Where: LVCCW Level 1 Hall 2 604 (Appsec Village) POD 2 - [Map](#)

Description:

Think you know AI pentesting? Put it to the test at this fast-paced, interactive trivia session at AppSec Village. AI Pentesting Trivia Showdown challenges participants with questions spanning offensive security fundamentals, real-world attack paths, AI-assisted testing concepts, vulnerability validation, and modern application security practices. Designed for practitioners of all experience levels, the game blends learning with competition in a format that is approachable, engaging, and fun to watch or join. Attendees will sharpen their understanding of how AI is changing penetration testing, pick up practical security insights, and leave with a stronger grasp of modern offensive techniques and terminology.

Speakers: Andy Dennis, Bill Reyor

SpeakerBio: Andy Dennis, Head of Field Engineering at XBOW

No BIO available

SpeakerBio: Bill Reyor

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: AI Pentesting Trivia Showdown

Tags: AppSec Village | Creator Event/Activity || All Audiences

When: Friday, Aug 7, 15:00 - 16:59 PDT

Where: LVCCW Level 1 Hall 2 604 (Appsec Village) POD 2 - [Map](#)

Description:

Think you know AI pentesting? Put it to the test at this fast-paced, interactive trivia session at AppSec Village. AI Pentesting Trivia Showdown challenges participants with questions spanning offensive security fundamentals, real-world attack paths, AI-assisted testing concepts, vulnerability validation, and modern application security practices. Designed for practitioners of all experience levels, the game blends learning with competition in a format that is approachable, engaging, and fun to watch or join. Attendees will sharpen their understanding of how AI is changing penetration testing, pick up practical security insights, and leave with a stronger grasp of modern offensive techniques and terminology.

Speakers: Andy Dennis, Bill Reyor

SpeakerBio: Andy Dennis, Head of Field Engineering at XBOW

No BIO available

SpeakerBio: Bill Reyor

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: AI Pentesting Trivia Showdown

Tags: AppSec Village | Creator Event/Activity || All Audiences

When: Saturday, Aug 8, 15:00 - 16:59 PDT

Where: LVCCW Level 1 Hall 2 604 (Appsec Village) POD 3 - [Map](#)

Description:

Think you know AI pentesting? Put it to the test at this fast-paced, interactive trivia session at AppSec Village. AI Pentesting Trivia Showdown challenges participants with questions spanning offensive security fundamentals, real-world attack paths, AI-assisted testing concepts, vulnerability validation, and modern application security practices. Designed for practitioners of all experience levels, the game blends learning with competition in a format that is approachable, engaging, and fun to watch or join. Attendees will sharpen their understanding of how AI is changing penetration testing, pick up practical security insights, and leave with a stronger grasp of modern offensive techniques and terminology.

Speakers: Andy Dennis, William Reyor

SpeakerBio: Andy Dennis, Head of Field Engineering at XBOW

No BIO available

SpeakerBio: William Reyor

Bill Reyor is a Lead Solutions Architect at XBOW, where he helps organizations evaluate and adopt autonomous offensive security testing to find exploitable application-layer vulnerabilities at scale. He has over 15 years of security experience spanning penetration testing, incident response, DevSecOps, application security leadership, and security program design, and is a co-author of O'Reilly's Defensive Security Handbook.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: AI Pipeline for N-days Weaponization

Tags: AI | DEF CON Demo Labs | Intermediate | Offense/Red Team | DEF CON Demo Labs

When: Friday, Aug 7, 11:00 - 11:45 PDT

Where: LVCCW Level 1 Hall 3 902 (Demo Labs Track 6) - [Map](#)

Description:

Most agentic exploit pipelines stall when there's no public PoC, they search, find nothing, and spin. This talk demos a multi-agent system that exploits n-days from scratch in under an hour, even with zero public exploit code available. Given only a CVE ID, the pipeline autonomously: fetches vulnerability details and the upstream fix commit; spins up a pinned Docker lab running the exact vulnerable version; diffs the patch to identify the exploitable code path; generates vulnerability-class-specific attack guidance (not a generic checklist); and runs iterative exploit + validation loops until RCE is confirmed. Demonstrated live against four CVSS 9.8–10.0 vulnerabilities Apache OpenMeetings deserialization, n8n unauthenticated RCE, Langflow exec() injection, and Spring AI SpEL injection, with working exploits produced in minutes. Every run also outputs a containerized lab and defense report, making it equally useful for detection engineering and patch validation.

Speakers: Andrea Brosio, Arun Nair

SpeakerBio: Andrea Brosio

Andrea Brosio is a Security Researcher and Senior Content Engineer at TryHackMe, specializing in red teaming, malware development, and offensive security. With prior experience as a Bug Hunter and Red Team Operator he combines real-world adversarial expertise with a passion for creating engaging cybersecurity training.

SpeakerBio: Arun Nair

Arun Nair is a Security Engineer at Google and founder of Ryvane Academy, specializing in AI Security, malware development, defense evasion, and adversary simulation. He holds several respected certifications, including OSCP, CRTP, CRTL, CodeMachine Malware Techniques, and HackSys Windows Kernel Exploitation. Over the years, Arun has worked with leading organizations such as JP Morgan, and EY, focusing on offensive security and red teaming engagements. Outside of his professional work, he is an active contributor to the cybersecurity community, from designing Capture the Flag (CTF) challenges to delivering talks and workshops at events like DEFCON Red Team Village, HeapCon, MCTTP, BSides Transylvania, HackSpaceCon, RingZero, c0c0n, and various local meetups. When he's not on engagements or speaking at conferences, Arun shares his research and insights through his blog at dazzyddos.github.io

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: AI Pipeline for N-days Weaponization

Tags: AI | DEF CON Demo Labs | Intermediate | Offense/Red Team | DEF CON Demo Labs

When: Saturday, Aug 8, 15:00 - 15:45 PDT

Where: LVCCW Level 1 Hall 3 902 (Demo Labs Track 6) - [Map](#)

Description:

Most agentic exploit pipelines stall when there's no public PoC, they search, find nothing, and spin. This talk demos a multi-agent system that exploits n-days from scratch in under an hour, even with zero public exploit code available. Given only a CVE ID, the pipeline autonomously: fetches vulnerability details and the upstream fix commit; spins up a pinned Docker lab running the exact vulnerable version; diffs the patch to identify the exploitable code path; generates vulnerability-class-specific attack guidance (not a generic checklist); and runs iterative exploit + validation loops until RCE is confirmed. Demonstrated live against four CVSS 9.8–10.0 vulnerabilities Apache OpenMeetings deserialization, n8n unauthenticated RCE, Langflow exec() injection, and Spring AI SpEL injection, with working exploits produced in minutes. Every run also outputs a containerized lab and defense report, making it equally useful for detection engineering and patch validation.

Speakers: Andrea Brosio, Arun Nair

SpeakerBio: Andrea Brosio

Andrea Brosio is a Security Researcher and Senior Content Engineer at TryHackMe, specializing in red teaming, malware development, and offensive security. With prior experience as a Bug Hunter and Red Team Operator he combines real-world adversarial expertise with a passion for creating engaging cybersecurity training.

SpeakerBio: Arun Nair

Arun Nair is a Security Engineer at Google and founder of Ryvane Academy, specializing in AI Security, malware development, defense evasion, and adversary simulation. He holds several respected certifications, including OSCP, CRTP, CRTL, CodeMachine Malware Techniques, and HackSys Windows Kernel Exploitation. Over the years, Arun has worked with leading organizations such as JP Morgan, and EY, focusing on offensive security and red teaming engagements. Outside of his professional work, he is an active contributor to the cybersecurity community, from designing Capture the Flag (CTF) challenges to delivering talks and workshops at events like DEFCON Red Team Village, HeapCon, MCTTP, BSides Transylvania, HackSpaceCon, RingZero, c0c0n, and various local meetups. When he's not on engagements or speaking at conferences, Arun shares his research and insights through his blog at dazzyddos.github.io

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: AI Safety Theater: What the RAISE Act Regulates — and What It Does Not

Tags: Policy @ DEF CON | Creator Talk/Panel

When: Saturday, Aug 8, 17:00 - 17:30 PDT

Where: LVCCW Level 1 Hall 3 801 (Creator Stage 1) - [Map](#)

Description:

New York's RAISE Act is among the most significant state AI safety laws in the country. Signed December 19, 2025, it imposes transparency requirements, safety plans, 72-hour incident reporting, and annual audits on frontier AI developers. It took effect 8 days after a presidential executive order authorizing the DOJ to challenge state AI laws. This talk applies the security researcher's methodology: map the surface, find the gaps, assess whether compliance cost is proportionate to actual risk reduction. The structural gaps are specific. The \$500M revenue threshold excludes the most aggressive AI capability development — well-capitalized but pre-revenue. The 10^2 FLOPs definition may not capture dangerous fine-tuned derivatives of frontier models. The catastrophic harm threshold requires 100+ deaths before reporting obligations attach — the alarm fires after the building has already burned. And the law requires transparency, not prohibition: a fully compliant developer can keep operating a system causing significant sub-catastrophic harm. 12 or more states are expected to model AI legislation on New York and California in 2026. If the security community does not engage critically with what this law actually does, those copies will inherit its gaps.

SpeakerBio: Joshua Marpet, Finite State

Joshua Marpet is Senior Product Security Consultant at Finite State, co-host of Paul's Security Weekly and Security Weekly News, and a CMMC co-author. He holds membership on the IEEE/UL 2933 and SPDX standards committees and serves on the boards of BSidesDE, Skytalks, and the Value Chain Risk Institute. A former police officer, firefighter, and Federal Reserve Bank of Philadelphia security analyst, he works at the intersection of security standards, policy, and operational practice.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

DEF CON Training - Tuesday - 08:30-17:30 PDT

Title: AI SecureOps: Attacking & Defending AI Applications & Agents

Tags: DEF CON Training (Paid) (2-day) | DEF CON Training

When: Tuesday, Aug 11, 08:30 - 17:30 PDT

Where: LVCCW Level 2 W228 (Workshops) - [Map](#)

Description:

SpeakerBio: Abhinav Singh

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

DEF CON Training - Monday - 08:30-17:30 PDT

Title: AI SecureOps: Attacking & Defending AI Applications & Agents

Tags: DEF CON Training (Paid) (2-day) | DEF CON Training

When: Monday, Aug 10, 08:30 - 17:30 PDT

Where: LVCCW Level 2 W228 (Workshops) - [Map](#)

Description:

SpeakerBio: Abhinav Singh

No BIO available



[Return to Index](#) - Add to Google

- ics [Calendar](#) file

Blue Team Village - Saturday - 14:30-15:30 PDT

Title: AI Security: Hype, Hacks, and the Future of Defense

Tags: Blue Team Village | Creator Talk/Panel

When: Saturday, Aug 8, 14:30 - 15:30 PDT

Where: LVCCW Level 2 W217 (Blue Team Village) Main Stage - [Map](#)

Description:

It starts with a simple prompt.

An AI assistant writes production code in seconds. A phishing email becomes nearly indistinguishable from a legitimate one. A security analyst uses an AI copilot to investigate hundreds of alerts—while an attacker uses the same technology to automate reconnaissance, create malware, and scale attacks.

Welcome to the new reality of cybersecurity.

AI is changing how we build, defend, attack, and trust technology. As organizations rapidly deploy AI applications and autonomous agents, defenders face two urgent questions: How can we use AI to defend better, and how do we secure AI itself?

Join AI and cybersecurity practitioners for an honest discussion that separates hype from reality. Through real-world stories and practical insights, we'll explore how attackers are using AI, how defenders are responding, what it means to secure AI systems, and where the industry is headed next.

Whether you're a seasoned blue teamer, security leader, AI enthusiast, or new to cybersecurity, you'll leave with a clearer view of today's AI security landscape—and what tomorrow's defenders need to know.

The future of cybersecurity is already here. Are you ready?

Speakers: Karan Dwivedi, Thomas Roccia, Todd Fletcher

SpeakerBio: Karan Dwivedi

Karan Dwivedi is a recognized cybersecurity expert. Currently, he serves as a security engineering manager at Google. Karan has led large-scale security projects at Google and Yahoo in the US for products like Google Search, Google Assistant, Yahoo Mail, Yahoo Finance, Flickr, etc, to safeguard over a billion users. At Yahoo, he was part of the security team responding to the world's largest data breach. He is the author of the book "Kickstart your security engineering career" which is a definitive guide for anyone looking to start a career in security engineering. Karan contributed to the latest internet standard for scoring vulnerabilities, the Common Vulnerability Scoring System (CVSS 4.0). He is featured in major media like Hakin9 Media Magazine, Forensic Focus News, etc. He has delivered talks at national and international conferences like Tech Ex North America, Tech Summit SF, BSides Las Vegas, National Cyber Summit, etc, to influence private and public sectors. Karan was featured as a subject matter expert in the Google Cybersecurity Certificate program launched in May 2023 on Coursera, which had an enrollment of over 41000 students in a few weeks. Furthermore, Karan has served as an advisor to startups, an editorial board member in international security journals, and judged global competitions. He holds a master's degree in Information Security from Carnegie Mellon University, USA. His portfolio can be found at <https://karand.me>

SpeakerBio: Thomas Roccia

Thomas Roccia is the Founder and Threat Researcher at SecurityBreak, a company dedicated to AI Threat Intelligence and AI security. With more than 15 years of experience in cybersecurity, he has investigated major cyberattacks, led threat research at Microsoft and McAfee, collaborated with law enforcement, and helped organizations understand and respond to emerging

threats.

Speaker / Contributor: This individual participates in SANS events, presentations, written content, or other community resources as an external contributor. They are not a SANS employee, instructor, or affiliate.

Since 2022, Thomas has focused on AI Threat Intelligence, researching how attackers target AI systems and how defenders can secure the growing AI ecosystem. He is recognized as one of the early pioneers in applying generative AI to cyber threat intelligence through practical research, open-source projects, and industry education.

Thomas is the creator of several widely used open-source initiatives, including the Unprotect Project and NOVA, one of the first detection-rule frameworks for prompt pattern matching and AI security monitoring. NOVA won the SANS AI Cybersecurity Hackathon in 2025, and Thomas received the SANS Difference Makers Award (DMA) the same year for his contributions to the cybersecurity community. He is also the author of the bestselling book Visual Threat Intelligence: An Illustrated Guide for Threat Researchers, recipient of the Bronze Foreword INDIES Award in the Science & Technology category.

A regular speaker at leading security conferences, including BlackHat, DEFCON, BSides, and SANS events, Thomas teaches AI Threat Intelligence to security professionals around the world, to help defenders apply AI to real-world investigations while understanding the risks attackers pose to the AI ecosystem.

Through SecurityBreak, Thomas develops research, intelligence, and products that help organizations monitor, detect, and defend against attacks targeting AI models, agents, tools, and the broader AI ecosystem.

SpeakerBio: Todd Fletcher

Todd Fletcher (@kobaltfox) has spent 25 years on the defense side, running IT and security for public government, wiring up SIEM and SOAR pipelines, and building security programs that survive contact with a real budget. He works at CrowdStrike as an AI Services Technical Lead in Strategic Advisory Services, where a lot of his job is separating what AI actually does for a SOC from what the slide deck claims it does.

He is also a PhD candidate in cyberpsychology at Birmingham City University (UK), studying the people doing the defending: what drives them, what burns them down, and why "humans are the weakest link" has always been a lazy answer. He writes at kobaltfox.com and toddmfletcher.com which starts from the position that defender mental health is a security outcome, not a wellness perk.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Contests - Saturday - 10:00-17:59 PDT

Title: AI Village - Hal CTF

Tags: AI Village | HALctf (AI Village CTF) | Contest

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 2 603 (AI Village) - [Map](#)

Description:

Get ready for the next evolution of competitive hacking at DEFCON 34! The AI Village is thrilled to introduce HalCTF (Hostile Autonomous Layer CTF), a first-of-its-kind agentic security competition. Instead of focusing on frontier models, this CTF is designed around how far you can stretch small local models that almost everyone can run. The first place prize is a DGX Spark so that you can continue your local hacking agent journey at home.

In this high-stakes arena, participants do not interact with targets directly. Instead, you will design and deploy autonomous AI agents programmed to navigate sandboxed environments, exploit challenge targets, and capture flags entirely on their own. Instead of just a prompt, we're asking for full containers that you can load up with all the tools you need to succeed.

To make it easy we're hosting everything, from the targets to your agents to the models. We have a mix of old and new, and you get more points if you use smaller models. Runs are quick and show you all of the logs and points so you can improve the agent over the course of the con.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Contests - Sunday - 10:00-13:59 PDT

Title: AI Village - Hal CTF

Tags: AI Village | HALctf (AI Village CTF) | Contest

When: Sunday, Aug 9, 10:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 2 603 (AI Village) - [Map](#)

Description:

Get ready for the next evolution of competitive hacking at DEFCON 34! The AI Village is thrilled to introduce HalCTF (Hostile Autonomous Layer CTF), a first-of-its-kind agentic security competition. Instead of focusing on frontier models, this CTF is designed around how far you can stretch small local models that almost everyone can run. The first place prize is a DGX Spark so that you can continue your local hacking agent journey at home.

In this high-stakes arena, participants do not interact with targets directly. Instead, you will design and deploy autonomous AI agents programmed to navigate sandboxed environments, exploit challenge targets, and capture flags entirely on their own. Instead of just a prompt, we're asking for full containers that you can load up with all the tools you need to succeed.

To make it easy we're hosting everything, from the targets to your agents to the models. We have a mix of old and new, and you get more points if you use smaller models. Runs are quick and show you all of the logs and points so you can improve the agent over the course of the con.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Contests - Friday - 10:00-17:59 PDT

Title: AI Village - Hal CTF

Tags: AI Village | HALctf (AI Village CTF) | Contest

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 2 603 (AI Village) - [Map](#)

Description:

Get ready for the next evolution of competitive hacking at DEFCON 34! The AI Village is thrilled to introduce HalCTF (Hostile Autonomous Layer CTF), a first-of-its-kind agentic security competition. Instead of focusing on frontier models, this CTF is designed around how far you can stretch small local models that almost everyone can run. The first place prize is a DGX Spark so that you can continue your local hacking agent journey at home.

In this high-stakes arena, participants do not interact with targets directly. Instead, you will design and deploy autonomous AI agents programmed to navigate sandboxed environments, exploit challenge targets, and capture flags entirely on their own. Instead of just a prompt, we're asking for full containers that you can load up with all the tools you need to succeed.

To make it easy we're hosting everything, from the targets to your agents to the models. We have a mix of old and new, and you get more points if you use smaller models. Runs are quick and show you all of the logs and points so you can improve the agent over the course of the con.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Contests - Sunday - 10:00-13:59 PDT

Title: AI Village Plays Pokemon: DEFCON Edition

Tags: AI Village | AI Village Plays Pokemon: DEF CON Edition | Contest

When: Sunday, Aug 9, 10:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 2 603 (AI Village) - [Map](#)

Description:

Agent harnesses and tooling have quickly become the AI buzzwords of 2026, but what do these even mean, and why should you consider building them? We're showing off how custom tooling can empower local models in the most accessible way possible: playing Pokémon. Join us in this fun, novice-friendly demo where we show how to build tooling for local models, and walk through what you should and shouldn't consider turning into tools. All the models and tools are open source, so feel free to use them to make your own agents to play our emulations of Pokémon Fire Red and Leaf Green.

SpeakerBio: Nick Ashworth, Maker at AI Village

Nick is a Hacker and Engineer with almost 15 years of experience hacking everything from power grids to satellites for the DoD. He's presented and made demos for Aerospace, Car Hacking, ICS, and the AI Village for the past seven years. He currently helps lead the AI Village.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Contests - Friday - 10:00-17:59 PDT

Title: AI Village Plays Pokemon: DEFCON Edition

Tags: AI Village | AI Village Plays Pokemon: DEF CON Edition | Contest

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 2 603 (AI Village) - [Map](#)

Description:

Agent harnesses and tooling have quickly become the AI buzzwords of 2026, but what do these even mean, and why should you consider building them? We're showing off how custom tooling can empower local models in the most accessible way possible: playing Pokémon. Join us in this fun, novice-friendly demo where we show how to build tooling for local models, and walk through what you should and shouldn't consider turning into tools. All the models and tools are open source, so feel free to use them to make your own agents to play our emulations of Pokémon Fire Red and Leaf Green.

SpeakerBio: Nick Ashworth, Maker at AI Village

Nick is a Hacker and Engineer with almost 15 years of experience hacking everything from power grids to satellites for the DoD. He's presented and made demos for Aerospace, Car Hacking, ICS, and the AI Village for the past seven years. He currently helps lead the AI Village.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Contests - Saturday - 10:00-17:59 PDT

Title: AI Village Plays Pokemon: DEFCON Edition

Tags: AI Village | AI Village Plays Pokemon: DEF CON Edition | Contest

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 2 603 (AI Village) - [Map](#)

Description:

Agent harnesses and tooling have quickly become the AI buzzwords of 2026, but what do these even mean, and why should you consider building them? We're showing off how custom tooling can empower local models in the most accessible way possible: playing Pokémon. Join us in this fun, novice-friendly demo where we show how to build tooling for local models, and walk through what you should and shouldn't consider turning into tools. All the models and tools are open source, so feel free to use them to make your own agents to play our emulations of Pokémon Fire Red and Leaf Green.

SpeakerBio: Nick Ashworth, Maker at AI Village

Nick is a Hacker and Engineer with almost 15 years of experience hacking everything from power grids to satellites for the DoD. He's presented and made demos for Aerospace, Car Hacking, ICS, and the AI Village for the past seven years. He currently helps lead the AI Village.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

The Diana Initiative - Saturday - 12:40-12:50 PDT

Title: AI Village Tour

Tags: The Diana Initiative | Creator Tour

When: Saturday, Aug 8, 12:40 - 12:50 PDT

Where: LVCCW Level 1 South Lobby / Atrium - [Map](#)

Description:

Interested in visiting AI Village but afraid to go by yourself? The Diana Initiative is hosting tours! Follow a volunteer to AI Village and be introduced to the community and activities inside!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

AI Village - Sunday - 12:30-12:59 PDT

Title: AI Village: Closing Remarks

Tags: AI Village | Creator Talk/Panel

When: Sunday, Aug 9, 12:30 - 12:59 PDT

Where: LVCCW Level 1 Hall 2 603 (AI Village) - [Map](#)

Description:



[Return to Index](#) - Add to Google - ics [Calendar](#) file

AI Village - Friday - 10:00-10:30 PDT

Title: AI Village: Opening Remarks

Tags: AI Village | Creator Talk/Panel

When: Friday, Aug 7, 10:00 - 10:30 PDT

Where: LVCCW Level 1 Hall 2 603 (AI Village) - [Map](#)

Description:



[Return to Index](#) - Add to Google - ics [Calendar](#) file

AI Village - Saturday - 10:00-17:59 PDT

Title: AI Village: Village Open

Tags: AI Village | Creator Event/Activity

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 2 603 (AI Village) - [Map](#)

Description:

We're bringing AI Village back to focus on what actually matters: practical, no-bullshit AI security. LLMs are an amazing technology, but they're not magic. We are stripping away the industry hype and focusing on hands-on skills, whether you are building your first exploit or leading an AI red team.

Here is what you can expect this year:

Drop-In Workshops: Walk up, grab a seat, and learn. We have drop in hands on mini-workshops on a bunch of topics. These include basic AI topics like how LLMs actually work, and how to build agents from scratch. For red teamers we have ones ranging from prompt injection to manipulating malware detection models. This is all running locally on a cluster we're bringing to DEF CON.

HalCTF: Our main competition this year will teach you how to write and fine-tune your own pentesting agent using open-source models. To handle the massive compute load, we're safely detonating these agents on GCP, giving each participant a dedicated GPU for their models.

Other Agent Shenanigans: The field moves fast and there's going to be something new by defcon. We're bringing a lot of compute to host things and we'll have some surprises in the space.

Whether you want to hear top-tier research from the people actually breaking these models or you just want to sit down and write an autonomous pentesting agent, we have the hardware and the labs ready for you.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: AI Village: Village Open

Tags: AI Village | Creator Event/Activity

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 2 603 (AI Village) - [Map](#)

Description:

We're bringing AI Village back to focus on what actually matters: practical, no-bullshit AI security. LLMs are an amazing technology, but they're not magic. We are stripping away the industry hype and focusing on hands-on skills, whether you are building your first exploit or leading an AI red team.

Here is what you can expect this year:

Drop-In Workshops: Walk up, grab a seat, and learn. We have drop in hands on mini-workshops on a bunch of topics. These include basic AI topics like how LLMs actually work, and how to build agents from scratch. For red teamers we have ones ranging from prompt injection to manipulating malware detection models. This is all running locally on a cluster we're bringing to DEF CON.

HalCTF: Our main competition this year will teach you how to write and fine-tune your own pentesting agent using open-source models. To handle the massive compute load, we're safely detonating these agents on GCP, giving each participant a dedicated GPU for their models.

Other Agent Shenanigans: The field moves fast and there's going to be something new by defcon. We're bringing a lot of compute to host things and we'll have some surprises in the space.

Whether you want to hear top-tier research from the people actually breaking these models or you just want to sit down and write an autonomous pentesting agent, we have the hardware and the labs ready for you.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: AI Village: Village Open

Tags: AI Village | Creator Event/Activity

When: Sunday, Aug 9, 10:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 2 603 (AI Village) - [Map](#)

Description:

We're bringing AI Village back to focus on what actually matters: practical, no-bullshit AI security. LLMs are an amazing technology, but they're not magic. We are stripping away the industry hype and focusing on hands-on skills, whether you are building your first exploit or leading an AI red team.

Here is what you can expect this year:

Drop-In Workshops: Walk up, grab a seat, and learn. We have drop in hands on mini-workshops on a bunch of topics. These include basic AI topics like how LLMs actually work, and how to build agents from scratch. For red teamers we have ones ranging from prompt injection to manipulating malware detection models. This is all running locally on a cluster we're bringing to DEF CON.

HalCTF: Our main competition this year will teach you how to write and fine-tune your own pentesting agent using open-source models. To handle the massive compute load, we're safely detonating these agents on GCP, giving each participant a dedicated GPU for their models.

Other Agent Shenanigans: The field moves fast and there's going to be something new by defcon. We're bringing a lot of compute to host things and we'll have some surprises in the space.

Whether you want to hear top-tier research from the people actually breaking these models or you just want to sit down and write an autonomous pentesting agent, we have the hardware and the labs ready for you.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: AI vs AI: Securing Telecom in the Era of Autonomous Cyber Warfare

Tags: Telecom Village | Creator Talk/Panel

When: Friday, Aug 7, 15:30 - 15:59 PDT

Where: LVCCW Level 3 W321 (Telecom Village) - [Map](#)

Description:

Key Discussion Points:

1. AI vs. AI Cyber Warfare: How AI is transforming both cyber defense and cyber offense in telecom, and whether autonomous attacks are already becoming a reality.
2. AI-Powered Telecom Security: The role of AI in SOC operations, fraud detection, threat intelligence, network security, and automated incident response.
3. Securing AI & AI Governance: Protecting AI models from threats such as prompt injection, data poisoning, model theft, and ensuring secure AI adoption through governance and human oversight.
4. Future of Telecom Security: AI-native networks, OEM and supply chain security, the evolution of security professionals, and preparing telecom operators for the AI-driven threat landscape by 2030.

Speakers: Rohini, Pankaj Sontakke, Will Thomas, Isabel Manjarrez, Omer Farooq, T-Mobile CTF Team, James (GSMA), Arvind Singh

SpeakerBio: Rohini

No BIO available

SpeakerBio: Pankaj Sontakke

No BIO available

SpeakerBio: Will Thomas

No BIO available

SpeakerBio: Isabel Manjarrez, Threat Researcher

[EN] María Isabel Manjarrez is a security researcher with Kaspersky's Global Research and Analysis Team (GReAT). She specializes in investigating threat actors in Latin America, tracking their movements, and analyzing the new techniques they deploy. She holds a degree in telecommunications and electronic systems engineering and her interests include threat intelligence, malware analysis, satellite communications, electronics, and music.

She has shared her knowledge as a speaker at local and international conferences such as Defcon, Security Analyst Summit (SAS), and EkoParty.

[ES] María Isabel Manjarrez es investigadora de seguridad en el Equipo Global de Investigación y Análisis (GReAT) de Kaspersky. Se especializa en la investigación de actores amenaza en Latinoamérica, rastrea sus movimientos y analiza las nuevas técnicas que implementan. Es Ingeniera en telecomunicaciones y sistemas electrónicos, sus intereses incluyen la inteligencia de amenazas, análisis de malware, comunicaciones satelitales, electrónica y música.

Ha compartido su conocimiento como ponente en conferencias locales e internacionales como Defcon, Security Analyst Summit (SAS) y EkoParty.

SpeakerBio: Omer Farooq

Omer Farooq is a cybersecurity, cloud, and artificial intelligence leader with more than twenty-five years of experience spanning application security, cloud architecture, software engineering, DevSecOps, AI security, and technology innovation. As Founder and Principal Security Consultant at Auxin Security, Omer has advised more than 100 organizations worldwide, including Fortune 500 companies, government agencies, healthcare organizations, and nonprofits. His expertise includes GenAI and LLM security, offensive security assessments, threat modeling, cloud security, DevSecOps transformation, secure software development, and enterprise architecture. Omer is a frequent speaker at industry conferences and events including

RSA Conference, BSides DC, AWS events, NAB Show, Microsoft Azure conferences, and numerous cybersecurity forums. His current research focuses on AI security, agentic systems, retrieval-augmented generation security, offensive AI testing, and emerging threats targeting enterprise AI deployments.

SpeakerBio: T -Mobile CTF Team
No BIO available

SpeakerBio: James(GSMA)
No BIO available

SpeakerBio: Arvind Singh
No BIO available

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: AI-assisted RF Hacking with GNU Radio

Tags: Radio Frequency Village | Creator Talk/Panel

When: Friday, Aug 7, 15:30 - 16:25 PDT

Where: LVCCW Level 1 Hall 1 409 (Radio Frequency Village) - [Map](#)

Description:

Software defined radios have lowered the barrier to RF experimentation, but GNU Radio still requires a working knowledge of blocks, port types, sample rates, hardware drivers, and connection rules. This talk presents an AI-assisted GNU Radio design system that lets a user describe an RF task in natural language, then uses a large language model to build, validate, and organize the resulting flowgraph through structured tool calls.

Direct LLM-generated GNU Radio code often looks plausible but fails in practice. Blocks may be incompatible, parameters may be invalid, connections may not match, and visual flowgraphs may be arranged in ways that make them difficult to inspect or modify. This system addresses those problems by exposing GNU Radio through validated tools for block discovery, hardware detection, flowgraph creation, parameter configuration, connection management, layout, and code generation. Before producing the final design, it checks port types, stream and message domains, vector lengths, and incompatible signal paths. When blocks cannot be connected directly, it recommends the required conversion blocks instead of generating a broken flowgraph.

This presentation will show the system live through practical SDR and RF security workflows. The goal is to make GNU Radio flowgraph development faster to use when exploring wireless systems, validating assumptions, and moving from an RF idea to a working flowgraph.

SpeakerBio: Erwin Karincic (Dollarhyde)

Erwin is an experienced security researcher specializing in both hardware and software reverse engineering, binary analysis, and exploit development across a range of processor architectures. He has notable experience in implementing complex Radio Frequency (RF) waveforms using Software Defined Radios (SDRs) for cybersecurity applications, complemented by his proficiency in designing, simulating, and fabricating antennas tailored for such applications. His past work includes extensive TCP/IP networking experience, designing worldwide secure communication systems. Erwin holds a number of prestigious certifications, including OSCP, OSCE, OSWE, OSEE, and CCIE Enterprise Infrastructure.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: AImaru C2: La Nueva Era del Living off the Land (MCP AI-Driven C2)

Tags: La Villa Community | Creator Talk/Panel

When: Friday, Aug 7, 13:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 4 1416 (La Villa Community) Main Stage - [Map](#)

Description:

¿Qué sucede cuando la barrera técnica para ejecutar ataques Living off the Land (LotL) desaparece y una IA toma el control?

Esta charla presenta AImaru C2, un framework ofensivo que expone el futuro del cibercrimen. AImaru introduce varios conceptos nuevos para la industria como la utilización del Model Context Protocol (MCP) para transformar clientes inofensivos en Troyanos de Acceso Remoto (RATs). Estos agentes usan binarios nativos del sistema para operar de forma encubierta, orquestados íntegramente por un LLM sin restricciones mediante lenguaje natural.

Demostremos cómo AImaru automatiza el cyberkill chain: desde bypasses dinámicos de AMSI generados al vuelo, jerarquización de tareas para Lotl, hasta la explotación de un vectores inéditos intenando abusar de IDEs locales (como Claude Code o PyCharm) para ejecución silenciosa.

Analizaremos cómo esto revolucionará el ecosistema RaaS/MaaS y los severos desafíos que enfrentarán los equipos de respuesta ante esta nueva generación de amenazas autónomas.

SpeakerBio: Mario Lobo, Cyber Threat Intelligence Researcher

I am a Colombian Cybersecurity Engineer with a Master's degree and a deep passion for the field. I have spent over 18 years immersed in various domains of Information Security and Cyber Intelligence.

My career has spanned critical sectors, including National Defense, where I spent nearly 10 years collaborating with Strategic Cyber Intelligence teams worldwide. I have led multiple cybersecurity teams for multinational banking institutions within the financial sector, and for several years now, I have served as the Lead Threat Intelligence Researcher at Lumu Technologies. I have been a main track speaker at prestigious international conferences such as Ekoparty, 8.8 Gob, BSides São Paulo, BSides Colombia, and Cyberwings, among others.

Beyond the professional realm, I am a guitar enthusiast, a dedicated cyclist, and a consummate music lover.

--

Soy colombiano, Ingeniero Magister en Ciberseguridad y un apasionado por el tema. Llevo más de 18 años sumergido diferentes campos de la Seguridad de la Información y la Ciberinteligencia.

Mi trayectoria me ha permitido transitar por sectores como la Defensa Nacional, donde por casi 10 años colaboré con equipos de Ciberinteligencia Estratégica alrededor del mundo. Lideré diferentes equipos de ciberseguridad para la banca multinacional en el sector Financiero y desde hace algunos años me desempeño como Lider Investigador de Inteligencia de Amenazas en Lumu Technologies. He participado como conferencista main track en eventos como Ekoparty, 8.8 Gob, BSides Sao Paulo y BSides Colombia, Cyberwings entre otros.

Fuera del ámbito profesional, soy un amante de la guitarra, la bici y un melómano consumado.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file



Title: AIMARU C2: The New Era of LotL (MCP AI-Driven C2)

Tags: Red Team Village | Misc

When: Saturday, Aug 8, 14:00 - 15:59 PDT

Where: LVCCW Level 1 Hall 1 309 (Red Team Village) Tactic Table 3 - [Map](#)

Description:

Almaru C2 is the evolution of a concept sparked by an unsettling question: What happens when an attacker can execute advanced Living off the Land (LotL) attacks without being an expert? While traditional LotL requires a specialist to navigate complex environments, Almaru C2 changes the game. Evolving from a PoC into a sophisticated Red Team framework, it automates expert-level tradecraft by subverting Anthropic's Model Context Protocol (MCP). By weaponizing MCP clients, it transforms a standard context protocol into a functional, autonomous multi-level RAT that natively "speaks" PowerShell.

Almaru C2 was born out of a critical necessity to ground cybersecurity in reality. While the industry often distracts itself with over-engineered narratives and hype-driven threats that ignore actual ecosystem data, a far more pragmatic danger has been hiding in plain sight. This framework addresses the unsettling evolution of the "Expert Bottleneck": What happens when the sophisticated LotL tactics, once reserved for elite nation-state actors, are democratized through automation? Named after the mythical serpent that glides unseen between the underworld and the land of the living, Almaru C2 represents the shift from manual expertise to autonomous execution. It is no longer just a proof of concept; it is a full-scale Red Team framework designed to expose how easily an unskilled attacker can now weaponize authorized system protocols to orchestrate advanced, data-driven breaches that traditional defenses simply aren't looking for.

To understand its impact, context is key. For years, LotL attacks have been the dominant tactic in ransomware campaigns. Instead of deploying traditional malware, threat actors abuse legitimate OS tools—such as PowerShell, WMI, or Certutil—to operate under the radar. In 2025, 82% of successful breaches were fileless or malwareless, with PowerShell ranking as the second most utilized TTP by groups like Black Basta, Royal, and LockBit.

This robust framework moves beyond experimental concepts, consolidating itself as a production-ready offensive platform. Almaru C2 is engineered with a modular architecture that prioritizes cryptographic integrity, operational security, and intelligent automation.

Core Framework Capabilities:

- **Model Context Protocol (MCP) RAT Engine:** A paradigm shift in command and control that subverts Anthropic's MCP from a standard context-sharing tool into a functional, undetectable Remote Access Trojan (RAT), tunneling all C2 traffic through legitimate LLM API communication.
- **PowerShell Client Builder:** An automated obfuscation engine featuring deep variable randomization and structural mutation to break static signatures.
- **AMSI Bypass Generator:** Dynamic generation of multi-stage bypass scripts, utilizing diverse techniques to neutralize the Antimalware Scan Interface in real-time.
- **Real-time Monitoring:** Advanced telemetry for live command execution tracking and granular session management.
- **Cryptographic Isolation:** Implementation of per-client encryption keys derived via HKDF-SHA256, ensuring that the compromise of one beacon does not jeopardize the entire fleet.
- **RBAC:** Native Role-Based Access Control, strictly segregating permissions between Admins, Users, and Viewers.
- **Complete Audit Logging:** Forensic-grade command history with millisecond-accurate timestamps for post-operation deconfliction.

By utilizing a multi-tier decision logic, the system dynamically selects and rewrites payloads based on the specific operational objective. This allows the C2 to scale its complexity in real-time—transitioning from basic PowerShell structures and stealthy WMI manipulation to the strategic abuse of LOLBins for high-complexity tasks. This adaptive approach ensures that every command utilizes the most effective legitimate system tool, successfully evading environment-specific defenses by blending into the target's unique operational noise.

Tactic Description: In this interactive session, attendees will sit down with the developer to operate the Almaru C2 framework in a controlled lab environment. Participants will experience the "Natural Language Intent" paradigm shift firsthand, moving away from manual syntax to intent-based exploitation.

Deployment: Deploy a lightweight MCP-Client on a target Windows machine and establish a beacon back to the AI-C2 controller.

Intent-Based Recon: Issue high-level natural language prompts (e.g., "Find sensitive PDF files and identify lateral movement paths") and observe the LLM selecting and generating the appropriate PowerShell/WMI code in real-time.

Automated Evasion: Trigger the Adaptive AMSI Bypass module, witnessing how the framework re-writes its own memory-resident payloads to evade active defenses.

All the technical information about the project is here: <https://github.com/mloborom/aimaru-c2>

SpeakerBio: Mario Lobo, Cyber Threat Intelligence Researcher

I am a Colombian Cybersecurity Engineer with a Master's degree and a deep passion for the field. I have spent over 18 years immersed in various domains of Information Security and Cyber Intelligence.

My career has spanned critical sectors, including National Defense, where I spent nearly 10 years collaborating with Strategic Cyber Intelligence teams worldwide. I have led multiple cybersecurity teams for multinational banking institutions within the financial sector, and for several years now, I have served as the Lead Threat Intelligence Researcher at Lumu Technologies. I have been a main track speaker at prestigious international conferences such as Ekoparty, 8.8 Gob, BSides São Paulo, BSides Colombia, and Cyberwings, among others.

Beyond the professional realm, I am a guitar enthusiast, a dedicated cyclist, and a consummate music lover.

--

Soy colombiano, Ingeniero Magister en Ciberseguridad y un apasionado por el tema. Llevo más de 18 años sumergido diferentes campos de la Seguridad de la Información y la Ciberinteligencia.

Mi trayectoria me ha permitido transitar por sectores como la Defensa Nacional, donde por casi 10 años colaboré con equipos de Ciberinteligencia Estratégica alrededor del mundo. Lideré diferentes equipos de ciberseguridad para la banca multinacional en el sector Financiero y desde hace algunos años me desempeño como Lider Investigador de Inteligencia de Amenazas en Lumu Technologies. He participado como conferencista main track en eventos como Ekoparty, 8.8 Gob, Bsides Sao Paulo y Bsides Colombia, Cyberwings entre otros.

Fuera del ámbito profesional, soy un amante de la guitarra, la bici y un melómano consumado.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: AIRGAP BREACHED: Monitoring the Ancestral Payload Leaking from the Poles

Tags: Biohacking Village | Creator Talk/Panel

When: Saturday, Aug 8, 15:00 - 15:30 PDT

Where: LVCCW Level 1 Hall 3 1104 (Creator Stage 4) - [Map](#)

Description:

A frugal, eDNA sniffing system to audit atmospheric biodata-leaks in the era of Climate change.

Current healthcare cybersecurity focuses on device access, ignoring the fundamental vulnerability: the environmental air gap is closing. Massive cryospheric melting is releasing a backlog of ancestral genetic data (eDNA) into the biosphere, creating an unmonitored 'input stream' of allergens and pathogens. This talk presents a resilient, open-source eDNA monitoring system designed to audit these atmospheric 'data leaks' in real-time. By utilizing high-fidelity open-source and decentralized brewed polymerases and consumer electronics, we provide a solution for biological sovereignty that remains operational even when traditional digital infrastructure fails.

Here, we will present how to build global atmospheric monitoring networks for under \$500 USD to intercept "paleo-organisms"—dormant bacteria and viruses released by melting poles—using shotgun metagenomics, 3D-printed parts, and microcontrollers. Essentially, he catches genetic ghosts in the air before they trigger the next global health crisis. This projects aims to tackle a sci-fi level threat: Facing the looming ecological danger of "polar amplification," David is developing open-source hardware together with Biohackers at BioOlympia (Olympia Washington), to capture and sequence ancient or threatening environmental DNA (eDNA). His atmospheric biosensors combine high-precision 3D printing, fluid dynamics, and embedded systems to track clouds of paleo-biomass and frozen microorganisms waking up from the ice or perturbed ecosystems. Along with studies in environmental science, biology, and Geographic Information systems, BioOlympia also operates a fully equipped BSL-2 research environment.

SpeakerBio: David J. Castillo-Cornejo

David is a biomedical scientist with experiences at the Max Planck Institute, Osaka University and ASU. He is the founder of Glyxon Biolabs. BioOlympia is a [Bio]Punk laboratory. The lab conducts advanced research in mammalian cell biology, CRISPR-based gene editing, and regenerative medicine.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Alerts and Warnings in 2026 Elections

Tags: Voting Village | Creator Talk/Panel

When: Saturday, Aug 8, 15:30 - 15:59 PDT

Where: LVCCW Level 2 W220 (Voting Village) (Voting Village Talks) - [Map](#)

Description:

The landscape supporting election cybersecurity has shifted dramatically since 2024. The federal government has lost most of its institutional knowledge about election security. Federal agencies have withdrawn from this space and diminished support for the Election Infrastructure Information Sharing and Analysis Center, leaving election officials and their vendors to shoulder the cybersecurity burden on their own. State and local election officials describe a breakdown in trust, reduced support, less intelligence, and other caustic effects that are debilitating the information-sharing environment. Meanwhile, advanced threats and threat actors have not gone away.

The fracturing of election security support goes beyond funding cuts for threat monitoring and fewer cyber assessments. Breakdowns in the multilateral information sharing mean that election officials lose early warnings, resource-strapped jurisdictions lose collective knowledge, and, critically, the federal government loses the capability to detect foreign campaigns to interfere in US elections.

An ineffective information-sharing environment leaves state and local jurisdictions facing sophisticated adversaries and criminal organizations without collective defense. Some losses can be replicated, but the gaps leave election security weaker than before.

Civil society, particularly former federal, state, and local election security professionals, is attempting to fill these gaps. Organizations such as the Election Security Exchange, Center for Democracy and Technology, Committee for Safe and Secure Elections, Partnership for Elections and Emergency Response, ASU Mechanics of Democracy Lab, MS-ISAC, Election Technology Education Fund, and other partners are rebuilding collective defenses. This panel acknowledges that the environment is what it is and demonstrates that vulnerabilities are not going unrecognized or unaddressed.

Speakers: Geoff Hale, Ryan Macias

SpeakerBio: Geoff Hale

Geoff Hale has over 15 years of experience supporting the security of critical infrastructure with a focus on election security since 2016. Geoff worked at the Cybersecurity and Infrastructure Security Agency (CISA) as Associate Director for Election Security & Resilience, helping to build a security community in support of U.S. elections.

SpeakerBio: Ryan Macias

Ryan Macias has spent over 20 years providing subject-matter expertise in election technology, security, and administration to election officials across the U.S. and election management bodies (EMBs) abroad. Macias has advised thousands of election stakeholders on strategies and methods to build resilience in election infrastructure, technology, and processes. Macias also teaches Election Security at the University of Minnesota and previously worked for the U.S. Election Assistance Commission (EAC) as the Acting Director of the Voting Systems Program and California Secretary of State, where he led the Top-to-Bottom Review of Voting Systems.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

IoT Village - Saturday - 10:00-17:59 PDT

Title: All About UART

Tags: IoT Village | Creator Workshop

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 215 (IoT Village) - [Map](#)

Description:

UART, it's in your smart camera, router, maybe even your phone and it's usually the easiest foothold into a device. In this hands-on workshop you'll learn to find it with a multimeter, read it with a logic analyzer...



[Return to Index](#) - Add to Google - ics [Calendar](#) file

IoT Village - Sunday - 10:00-13:59 PDT

Title: All About UART

Tags: IoT Village | Creator Workshop

When: Sunday, Aug 9, 10:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 1 215 (IoT Village) - [Map](#)

Description:

UART, it's in your smart camera, router, maybe even your phone and it's usually the easiest foothold into a device. In this hands-on workshop you'll learn to find it with a multimeter, read it with a logic analyzer...



[Return to Index](#) - Add to Google - ics [Calendar](#) file

IoT Village - Friday - 10:00-17:59 PDT

Title: All About UART

Tags: IoT Village | Creator Workshop

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 215 (IoT Village) - [Map](#)

Description:

UART, it's in your smart camera, router, maybe even your phone and it's usually the easiest foothold into a device. In this hands-on workshop you'll learn to find it with a multimeter, read it with a logic analyzer...



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: AMA with EFF

Tags: DCNextGen | Creator Talk/Panel | Youth

When: Saturday, Aug 8, 15:00 - 15:40 PDT

Where: LVCCW Level 3 W316 (DC NextGen) - [Map](#)

Description:

Learn about EFF's work protecting your right to send memes to your friends, watch videos online, and go outside without surveillance. Ask questions about EFF's work, from how we fight bad laws in Congress to how we take on big tech companies. Whether you're curious about technology, want to know how to protect your privacy, or just want to know what a nonprofit org actually does, this is your chance to ask us anything.

SpeakerBio: EFF

No BIO available

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: An Android voyage from Java to Smali with ASM

Tags: Mobile Hacking Community | Creator Talk/Panel

When: Saturday, Aug 8, 11:15 - 12:15 PDT

Where: LVCCW Level 1 Hall 4 1422 (Mobile Hacking Community) - [Map](#)

Description:

The Java programming language is the backbone of almost all Android applications, yet its compilation process is often discarded. Behind the scenes, a complex series of bytecode transformations takes place, and tools such as ASM allow anyone to hook into the process and alter the flow to achieve better performance, obfuscation, compile-time code injection, ... In this talk, we'll explore how this tool works, how it can be used, and the deep pitfalls to look out for when performing Java bytecode manipulation.

SpeakerBio: Ricardo Loura

No BIO available

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Malware Village - Saturday - 14:10-16:50 PDT

Title: An Intro to Mac Malware Analysis

Tags: Malware Village | Creator Workshop

When: Saturday, Aug 8, 14:10 - 16:50 PDT

Where: LVCCW Level 1 Hall 2 600 (Malware Village) Workshops - [Map](#)

Description:

Patrick has spent the past 20 years studying macOS malware, building tools to detect it, and authoring The Art of Mac Malware book series. In this training, you'll learn the tools and techniques needed to detect and analyze modern threats targeting Apple's desktop OS.

We'll cover common infection vectors, persistence mechanisms, and capabilities of macOS malware, along with an introduction to the tools and techniques used to classify and analyze malicious binaries.

SpeakerBio: Patrick Wardle, CEO and Co-Founder at DoubleYou

Patrick Wardle is the cofounder of the Objective-See Foundation, CEO and cofounder of DoubleYou, and author of The Art of Mac Malware series. He previously worked at NASA and the NSA, and has presented at countless security conferences, making him intimately familiar with aliens, spies, and talking nerdy.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Call Center Village - Friday - 15:00-15:59 PDT

Title: An Intrusion in the Living Room is now an international incident: SuperBOX Part 3

Tags: Call Center Village | Creator Talk/Panel

When: Friday, Aug 7, 15:00 - 15:59 PDT

Where: LVCCW Level 2 W218 (Call Center Village) - [Map](#)

Description:

Free cable box, or Chinese-controlled botnet node? Darknet Diaries Ep. 172 exposed SuperBox as both. Part 3 breaks down how one sketchy streaming device turned a living room into a national security case.

SpeakerBio: D3adA55

No BIO available

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

DEF CON Training - Tuesday - 08:30-17:30 PDT

Title: Analyze, Detect & Hunt: Hands-On Malware Analysis, Memory Forensics & AI-Driven Threat Hunting with Endpoint Telemetry

Tags: DEF CON Training (Paid) (2-day) | DEF CON Training

When: Tuesday, Aug 11, 08:30 - 17:30 PDT

Where: LVCCW Level 2 W215 Blue Team Village Main Room (CTF,The Nook & Mental Health Hackers) - [Map](#)

Description:

Speakers: Monnappa K A, Sajan Shetty

SpeakerBio: Monnappa K A

No BIO available

SpeakerBio: Sajan Shetty

No BIO available

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

DEF CON Training - Monday - 08:30-17:30 PDT

Title: Analyze, Detect & Hunt: Hands-On Malware Analysis, Memory Forensics & AI-Driven Threat Hunting with Endpoint Telemetry

Tags: DEF CON Training (Paid) (2-day) | DEF CON Training

When: Monday, Aug 10, 08:30 - 17:30 PDT

Where: LVCCW Level 2 W215 Blue Team Village Main Room (CTF,The Nook & Mental Health Hackers) - [Map](#)

Description:

Speakers: Monnappa K A, Sajan Shetty

SpeakerBio: Monnappa K A

No BIO available

SpeakerBio: Sajan Shetty

No BIO available

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Anatomy of a Sandworm: A Deep Dive into the Shai-Hulud Attacks

Tags: Malware Village | Creator Talk/Panel

When: Friday, Aug 7, 10:00 - 10:45 PDT

Where: LVCCW Level 1 Hall 2 600 (Malware Village) Talks - [Map](#)

Description:

Format: Talk

Length: 20-40min (I'm flexible, I can adjust the content based on how long the time slot is)

Abstract: In September 2025, an obscure npm package shipped with a piece of JavaScript that should not have been there. A new beast had emerged among supply chain attacks. Within 48 hours, that JavaScript had copied itself into more than 180 packages. It did something that hadn't been seen before in such an attack. It was self-propagating. It was a worm. And it was LOUD. Hundreds of public repos were created, littered with stolen secrets. Within nine days, it had triggered an emergency CISA alert.

Two months later, we witnessed the "Second Coming": a far more aggressive successor returned, racing a deadline npm itself had set, and leaving behind roughly 700 compromised packages, ~25,000 GitHub repositories of stolen secrets, and a destructive payload that wiped victims' home directories when it couldn't exfiltrate them. And these were just the first two attacks.

This talk is a technical breakdown of the Shai-Hulud worm family: the first malware to spread successfully through the npm ecosystem as a self-replicating worm, and the iterations that followed. We'll examine how the malware infected its victims, turned legitimate security tooling against them, what it stole, and how it kept spreading.

Each iteration evolved to defeat the defenses put in place against the last, swapping tools, tactics, and even its JavaScript runtime. Stranger still: the malware wasn't trying to hide. It branded its own exfiltration repositories, named its propagation functions clearly in source, and used victims' own GitHub accounts to share stolen secrets. By the end, we'll have a clearer picture of how these supply chain worms work, and what each rising of Shai-Hulud has taught us.

SpeakerBio: Megg Sage, AppSec engineer who explains scary things about your dependencies

Megg is an application security engineer who started out as a web developer. Security drew her in with the endless puzzles and challenges put forth by the field. She loves sharing knowledge, particularly when she can both educate and frighten her audience at the same time. After all, what can happen when security goes wrong is pretty scary. She also enjoys working closely with software engineering teams to try to make security work within existing development practices or at least minimize the pain of "doing security." When not behind a computer, Megg can usually be found making some sort of costume piece or shiny object.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Anomalies Are Not Normal: Election Foam Strikes and the Tragic Story of Mikey Hicks

Tags: Voting Village | Creator Talk/Panel

When: Friday, Aug 7, 11:00 - 11:30 PDT

Where: LVCCW Level 2 W220 (Voting Village) (Voting Village Talks) - [Map](#)

Description:

The last time I spoke at DEF CON's Voting Village, *Curling v. Raffensperger* was still awaiting a decision. Since then, the technical record has expanded, the litigation has largely run its course, and yet the strategic debate has changed remarkably little. High-consequence systems operate under two competing optimizations. Engineers optimize for reality. Administrators optimize for operations. Successful missions answer operational questions; they do not validate engineering assumptions. Yet documented engineering anomalies that do not lead to immediate mission failure gradually become accepted as normal. Researchers are repeatedly asked to demonstrate that documented engineering anomalies will produce catastrophic failure, while institutions are seldom asked to explain why anomalies have become compatible with normal operations. This burden-shifting has shaped two decades of election security research while limiting its strategic impact. The election security community has accepted the wrong burden. To the extent that security researchers participate in defining the safety boundaries of electronic election infrastructure, their role has largely been to discover and document anomalies and provide expert testimony in proceedings aimed at optimizing normal election operations. Lost in that process is the implication that "normal operation" has a factual, engineering basis. In practice, normality has become an institutional designation that researchers seldom contest. This talk argues that changing the burden fundamentally changes what institutions are permitted to call normal. It proposes a new research agenda focused less on discovering the next anomaly than on preventing documented engineering anomalies from becoming institutionalized as accepted practice. The implications extend well beyond elections. The forthcoming book *Sovereign Code* argues that the same organizational dynamics increasingly govern all software-mediated public administration. The success of the next generation of election security research will be measured not by the anomalies it discovers, but by the anomalies institutions are no longer able to call normal.

SpeakerBio: Richard DeMillo

Richard DeMillo holds the Charlotte B. and Roger C. Warren Chair in Computing at The Georgia Institute of Technology in Atlanta, Georgia. He is the former Dean of Georgia Tech's College of Computing, founding Chair of the School of Cybersecurity and Privacy, and founder of the Center for 21st Century Universities. In industry, he was previously Vice President and Chief Technology Officer for Hewlett-Packard, and General Manager and Head of Computing Research for Bellcore/SAIC. In government, he directed the Computer and Computation Research Division at the National Science Foundation and the Software Test and Evaluation Project for the Office of the Secretary of Defense. He is the author of more than 100 scientific articles, books, and patents in cryptography, cybersecurity, and software engineering. He is a fellow of the American Association for the Advancement of Science, the Association for Computing Machinery, and the Lumina Foundation.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Anyone Can Hack IoT (Even Easier Now) - A Beginner's Guide to AI Augmented IoT Hacking

Tags: IoT Village | Creator Talk/Panel

When: Saturday, Aug 8, 11:45 - 12:30 PDT

Where: LVCCW Level 1 Hall 3 1105 (Creator Stage 3) - [Map](#)

Description:

Two years ago I gave a popular talk at Defcon called "Anyone Can Hack IoT" and the message was simple, you don't need expensive gear and I can show you how. All of that is true, but now it's even easier and I want to show you why. Whether you saw the original talk or this is your first time thinking about IoT hacking, I'll show you how AI has actually made it even easier. In this talk I'll show you what's actually useful and what not by walking through my real workflow that I've used to find multiple CVEs. I'll demo Wairz, an open source tool I built that lets AI agents help reverse engineering firmware, along with some other hardware tools I've put together to give AI direct access to devices on my bench. I'll cover what's worth using AI for, what's still better done by hand and how you can build your own AI assisted setup at home and hack your first device (or second or third or so on).

SpeakerBio: Andrew Bellini

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: AOBTD: AI One Bites The DAST

Tags: Intro/Beginner | AI | DEF CON Demo Labs | AppSec | Offense/Red Team | DEF CON Demo Labs

When: Saturday, Aug 8, 15:00 - 15:45 PDT

Where: LVCCW Level 1 Hall 3 901 (Demo Labs Track 5) - [Map](#)

Description:

I hate the way most DAST tools test: firing payloads at parameters with no idea what the app is. They catch the obvious stuff, but miss the parts that actually need context. Newer LLM scanners are either commercial black boxes (iykyk) or "GPT, find bugs at this URL" wrappers that fall over outside a CTF box.

AOBTD is my attempt at a third option: a scanner that behaves less like a fuzzer and more like a pentester at the start of a test.

Instead of fuzzing harder, AOBTD first tries to understand the target. It explores the surface, identifies what pages and endpoints are for, takes notes, builds hypotheses, and then sends targeted requests based on that context. This target understanding drives the rest of the testing process, which is the only realistic way automated tooling can get closer to business-logic bugs.

The crawler is designed to avoid wasting time on repeated templates while still sampling outliers, so the odd page hidden in a sea of similar ones does not get ignored. When findings are confirmed, AOBTD can chain them into multi-step attack stories rather than reporting isolated payload hits.

This is where LLMs are actually useful: reading a page, understanding the purpose of a form, naming the function behind a JSON endpoint, and doing the kind of prioritization a pentester normally spends hours on.

SpeakerBio: Ozgun "ozzy" Kultekin

Ozgun (aka ozzy) is a Senior Application Security Engineer at Trendyol Group, where he spends his days breaking applications before the bad guys do. He holds the OSCE3 certification and specializes in offensive security research with a focus on application security and red team operations.

He has presented at several conferences including DEF CON, Hacktivity, and multiple BSides events, covering topics ranging from red teaming to application security. He is currently focused on integrating AI into offensive security workflows and actively researching how large language models can be applied in practical, technical ways within cybersecurity. He regularly shares his work and tools as open source.

When he's not hunting bugs or running red team ops, he's probably at the poker table.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: AOBTD: AI One Bites The DAST

Tags: Intro/Beginner | AI | DEF CON Demo Labs | AppSec | Offense/Red Team | DEF CON Demo Labs

When: Friday, Aug 7, 11:00 - 11:45 PDT

Where: LVCCW Level 1 Hall 3 901 (Demo Labs Track 5) - [Map](#)

Description:

I hate the way most DAST tools test: firing payloads at parameters with no idea what the app is. They catch the obvious stuff, but miss the parts that actually need context. Newer LLM scanners are either commercial black boxes (iykyk) or "GPT, find bugs at this URL" wrappers that fall over outside a CTF box.

AOBTD is my attempt at a third option: a scanner that behaves less like a fuzzer and more like a pentester at the start of a test.

Instead of fuzzing harder, AOBTD first tries to understand the target. It explores the surface, identifies what pages and endpoints are for, takes notes, builds hypotheses, and then sends targeted requests based on that context. This target understanding drives the rest of the testing process, which is the only realistic way automated tooling can get closer to business-logic bugs.

The crawler is designed to avoid wasting time on repeated templates while still sampling outliers, so the odd page hidden in a sea of similar ones does not get ignored. When findings are confirmed, AOBTD can chain them into multi-step attack stories rather than reporting isolated payload hits.

This is where LLMs are actually useful: reading a page, understanding the purpose of a form, naming the function behind a JSON endpoint, and doing the kind of prioritization a pentester normally spends hours on.

SpeakerBio: Ozgun "ozzy" Kultekin

Ozgun (aka ozzy) is a Senior Application Security Engineer at Trendyol Group, where he spends his days breaking applications before the bad guys do. He holds the OSCE3 certification and specializes in offensive security research with a focus on application security and red team operations.

He has presented at several conferences including DEF CON, Hacktivity, and multiple BSides events, covering topics ranging from red teaming to application security. He is currently focused on integrating AI into offensive security workflows and actively researching how large language models can be applied in practical, technical ways within cybersecurity. He regularly shares his work and tools as open source.

When he's not hunting bugs or running red team ops, he's probably at the poker table.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Contests - Friday - 10:00-23:59 PDT

Title: Apex Park (Cloud Village CTF)

Tags: Cloud Village | Apex Park (Cloud Village CTF) | Contest

When: Friday, Aug 7, 10:00 - 23:59 PDT

Where: LVCCW Level 3 W312 (Cloud Village CTF) - [Map](#)

Description:

Cloud Village CTF will be a jeopardy style 2 days contest where participants will have to solve challenges around Cloud infrastructure, security, recon, etc. These challenges will cover different cloud platforms including AWS, GCP, Azure, Digital Ocean, etc. We will also reward our top 3 teams with awards.““

Participant Prerequisites

A laptop with unfiltered internet access and an open mind to learn with the community.

Timing

Cloud Village CTF @ DEF CON 34: 7th & 8th August 2026 CTF starts - 7th August, 2026 - 10:00AM PDT CTF closes - 8th August 2026 - 23:59PM PDT CTF registrations opens - 30th July 2026 - 10:00AM PDT



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Contests - Saturday - 10:00-23:59 PDT

Title: Apex Park (Cloud Village CTF)

Tags: Cloud Village | Apex Park (Cloud Village CTF) | Contest

When: Saturday, Aug 8, 10:00 - 23:59 PDT

Where: LVCCW Level 3 W312 (Cloud Village CTF) - [Map](#)

Description:

Cloud Village CTF will be a jeopardy style 2 days contest where participants will have to solve challenges around Cloud infrastructure, security, recon, etc. These challenges will cover different cloud platforms including AWS, GCP, Azure, Digital Ocean, etc. We will also reward our top 3 teams with awards.““

Participant Prerequisites

A laptop with unfiltered internet access and an open mind to learn with the community.

Timing

Cloud Village CTF @ DEF CON 34: 7th & 8th August 2026 CTF starts - 7th August, 2026 - 10:00AM PDT CTF closes - 8th August 2026 - 23:59PM PDT CTF registrations opens - 30th July 2026 - 10:00AM PDT

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

DEF CON Training - Monday - 08:30-17:30 PDT

Title: Applied SDR Hacking: Red Team SIGINT for mission-critical, automotive, aviation, and marine targets

Tags: DEF CON Training (Paid) (2-day) | DEF CON Training

When: Monday, Aug 10, 08:30 - 17:30 PDT

Where: LVCCW Level 2 W231 (Workshops) - [Map](#)

Description:

Speakers: Jos Wetzels, Wouter Bokslag

SpeakerBio: Jos Wetzels, Midnight Blue

No BIO available

SpeakerBio: Wouter Bokslag, Midnight Blue

Wouter Bokslag is a co-founding partner and security researcher at Midnight Blue. He is known for the reverse-engineering and cryptanalysis of several proprietary in-vehicle immobilizer authentication ciphers used by major automotive manufacturers as well as co-developing the world's fastest public attack against the Hitag2 cipher. He holds a Master's Degree in Computer Science & Engineering from Eindhoven University of Technology (TU/e) and designed and assisted in teaching hands-on offensive security classes for graduate students at the Dutch Kerckhoffs Institute for several years.

Recently heavily involved in the TETRA:BURST research and associated follow-up research, such as the recent reverse-engineering and analysis of the elusive TETRA End-to-End protocol. Also, a contributor of open-source SDR code.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

DEF CON Training - Tuesday - 08:30-17:30 PDT

Title: Applied SDR Hacking: Red Team SIGINT for mission-critical, automotive, aviation, and marine targets

Tags: DEF CON Training (Paid) (2-day) | DEF CON Training

When: Tuesday, Aug 11, 08:30 - 17:30 PDT

Where: LVCCW Level 2 W231 (Workshops) - [Map](#)

Description:

Speakers: Jos Wetzels, Wouter Bokslag

SpeakerBio: Jos Wetzels, Midnight Blue

No BIO available

SpeakerBio: Wouter Bokslag, Midnight Blue

Wouter Bokslag is a co-founding partner and security researcher at Midnight Blue. He is known for the reverse-engineering and cryptanalysis of several proprietary in-vehicle immobilizer authentication ciphers used by major automotive manufacturers as well as co-developing the world's fastest public attack against the Hitag2 cipher. He holds a Master's Degree in Computer Science & Engineering from Eindhoven University of Technology (TU/e) and designed and assisted in teaching hands-on offensive security classes for graduate students at the Dutch Kerckhoffs Institute for several years.

Recently heavily involved in the TETRA:BURST research and associated follow-up research, such as the recent reverse-engineering and analysis of the elusive TETRA End-to-End protocol. Also, a contributor of open-source SDR code.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: AppSec Quiz Gauntlet: Spot the Vulnerability

Tags: AppSec Village | Creator Event/Activity || All Audiences

When: Sunday, Aug 9, 11:00 - 12:59 PDT

Where: LVCCW Level 1 Hall 2 604 (Appsec Village) POD 2 - [Map](#)

Description:

In AppSec Quiz Gauntlet: Spot the Vulnerability, you'll join a hands-on security quiz built around real-world software risks. Analyze suspicious dependencies, uncover typosquatted packages, decode obfuscated snippets, and identify hidden vulnerabilities in short code samples.

SpeakerBio: Avek Kolech

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: AppSec Quiz Gauntlet: Spot the Vulnerability

Tags: AppSec Village | Creator Event/Activity || All Audiences

When: Saturday, Aug 8, 15:00 - 16:59 PDT

Where: LVCCW Level 1 Hall 2 604 (Appsec Village) POD 2 - [Map](#)

Description:

In AppSec Quiz Gauntlet: Spot the Vulnerability, you'll join a hands-on security quiz built around real-world software risks. Analyze suspicious dependencies, uncover typosquatted packages, decode obfuscated snippets, and identify hidden vulnerabilities in short code samples.

SpeakerBio: Avek Kolech

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: AppSec Quiz Gauntlet: Spot the Vulnerability

Tags: AppSec Village | Creator Event/Activity || All Audiences

When: Saturday, Aug 8, 13:00 - 14:59 PDT

Where: LVCCW Level 1 Hall 2 604 (Appsec Village) POD 2 - [Map](#)

Description:

In AppSec Quiz Gauntlet: Spot the Vulnerability, you'll join a hands-on security quiz built around real-world software risks. Analyze suspicious dependencies, uncover typosquatted packages, decode obfuscated snippets, and identify hidden vulnerabilities in short code samples.

SpeakerBio: Avek Kolech

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: AppSec Quiz Gauntlet: Spot the Vulnerability

Tags: AppSec Village | Creator Event/Activity || All Audiences

When: Friday, Aug 7, 13:00 - 14:59 PDT

Where: LVCCW Level 1 Hall 2 604 (Appsec Village) POD 4 - [Map](#)

Description:

In AppSec Quiz Gauntlet: Spot the Vulnerability, you'll join a hands-on security quiz built around real-world software risks. Analyze suspicious dependencies, uncover typosquatted packages, decode obfuscated snippets, and identify hidden vulnerabilities in short code samples.

SpeakerBio: Avek Kolech

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

The Diana Initiative - Friday - 10:30-10:40 PDT

Title: AppSec Village Tour

Tags: The Diana Initiative | Creator Tour

When: Friday, Aug 7, 10:30 - 10:40 PDT

Where: LVCCW Level 1 South Lobby / Atrium - [Map](#)

Description:

Interested in visiting AppSec Village but afraid to go by yourself? The Diana Initiative is hosting tours! Follow a volunteer to AppSec Village and be introduced to the community and activities inside!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Social Gatherings/Events - Friday - 21:00-00:59 PDT

Title: Arcade Party

Tags: Party

When: Friday, Aug 7, 21:00 - 00:59 PDT

Where: LVCCW Level 1 Hall 3 801 (Creator Stage 1,2) - [Map](#)

Description:

The Arcade Party is back! Come play your favorite classic arcade games while jamming out to Keith Myers DJing. Your favorite custom built 16 player LED foosball table will be ready for some competitive games. This epic party, free for DEF CON 34 attendees to enjoy and play, is hosted by the Military Cyber Professionals Association (a tech ed charity) and friends.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Noob Community - Friday - 10:00-17:59 PDT

Title: Arcanum Security Labs

Tags: Noob Community | Creator Event/Activity

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 4 1417 (Noob Community) - [Map](#)

Description:

Arcanum Security delivers modern cybersecurity through cutting-edge training and consulting, led by Jason Haddix and crew, spanning offensive security, bug bounty hunting, and AI security. Stop by during village hours to work through their hands-on labs.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Noob Community - Sunday - 10:00-13:59 PDT

Title: Arcanum Security Labs

Tags: Noob Community | Creator Event/Activity

When: Sunday, Aug 9, 10:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 4 1417 (Noob Community) - [Map](#)

Description:

Arcanum Security delivers modern cybersecurity through cutting-edge training and consulting, led by Jason Haddix and crew, spanning offensive security, bug bounty hunting, and AI security. Stop by during village hours to work through their hands-on labs.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Noob Community - Saturday - 10:00-17:59 PDT

Title: Arcanum Security Labs

Tags: Noob Community | Creator Event/Activity

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 4 1417 (Noob Community) - [Map](#)

Description:

Arcanum Security delivers modern cybersecurity through cutting-edge training and consulting, led by Jason Haddix and crew, spanning offensive security, bug bounty hunting, and AI security. Stop by during village hours to work through their hands-on labs.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Are We Making Things Worse? Election Denialism and Security Research

Tags: Voting Village | Creator Talk/Panel

When: Saturday, Aug 8, 11:30 - 11:59 PDT

Where: LVCCW Level 2 W220 (Voting Village) (Voting Village Talks) - [Map](#)

Description:

Speakers: Matt Blaze, Geoff Hale, Michael Moore, Kendall Spencer, Philip Stark

SpeakerBio: Matt Blaze

Matt Blaze is the McDevitt chair in Computer Science and Law at Georgetown University, where he studies problems at the intersection of technology and public policy. Election systems and voting technology are central focuses of his research. He led teams as part of the California TTBR and Ohio EVEREST studies that each found deep and fundamental weaknesses in different election technologies used by those states and the rest of the US. He has testified on technical risks in elections before the US Congress and other bodies numerous times. Blaze is a co-founder of the Voting Village and president of the Election Integrity Foundation.

SpeakerBio: Geoff Hale

Geoff Hale has over 15 years of experience supporting the security of critical infrastructure with a focus on election security since 2016. Geoff worked at the Cybersecurity and Infrastructure Security Agency (CISA) as Associate Director for Election Security & Resilience, helping to build a security community in support of U.S. elections.

SpeakerBio: Michael Moore

Michael Moore is the CISO at Arizona Secretary of State's Office. He leads efforts to strengthen election security through coordinated partnerships across federal, state, and local governments, alongside trusted private-sector partners. His work is grounded in protecting democratic processes and maintaining public confidence in elections. He focuses on the most pressing risks to election integrity: mis-, dis-, and malinformation (MDM), and the insider threats that can emerge from an increasingly polarized and misinformed environment. His approach centers on countering false narratives with verifiable truth while advancing a defense-in-depth strategy. This includes preventing attacks wherever possible, rapidly detecting anomalies, and ensuring resilient, transparent recovery when incidents occur.

Through organizational leadership and national collaboration, Michael has driven initiatives that enhance the security, resilience, and credibility of election systems. His work helps safeguard the voter experience and uphold trust in democratic institutions.

SpeakerBio: Kendall Spencer

Kendall Spencer is an attorney specializing in emerging companies, technology transactions, and the legal issues shaping innovation. Since joining DEF CON's Voting Village as a Georgetown Law student in 2019, he has worked alongside Matt Blaze, David Jefferson, and the Voting Village team at the intersection of election technology, cybersecurity, and democracy. Spencer serves on the Board of Directors of the Election Integrity Foundation and has advised state election officials on election security, post-election audits, and cybersecurity best practices. His work focuses on bridging the gap between technical research, public policy, and the law—helping policymakers, election officials, security researchers, and the public better understand the role election security plays in strengthening democratic institutions and public confidence in elections. A frequent DEF CON speaker, Spencer is passionate about fostering thoughtful, bipartisan conversations on the role of technology in protecting election integrity and the democratic principles that underpin a free and open society. Outside of his legal and technology work, Spencer is a rare book dealer and collector specializing in early American history and the Black diaspora.

SpeakerBio: Philip Stark

Philip B. Stark is Distinguished Professor of the Graduate School at the University of California, Berkeley, where he has served as department chair and associate dean. In 2007 he invented "risk-limiting audits" ("RLAs"), endorsed by the National Academies of Science, Engineering, and Medicine and the American Statistical Association, among others, and required or authorized by law in about 15 states. He designed and helped conduct the first dozen pilot RLAs, helped draft RLA legislation for several states, and has published open-source software to support RLAs. In 2012, he and David Wagner introduced "evidence-based elections," a paradigm for conducting demonstrably trustworthy elections. Stark has served on the Board of Advisors of the US Election Assistance Commission and its cybersecurity subcommittee, the Board of Directors of Verified Voting Foundation and the Election Integrity Foundation, and on the California Post Election Audit Standards Working Group. He has worked with the Secretaries of State of California, Colorado, and New Hampshire and numerous local election officials. He has testified about election integrity in state and federal courts and to legislators. He received the IEEE Cybersecurity Award for Practice, the UC Berkeley Chancellor's Award for Research in the Public Interest, and the John Gideon Award for Election Integrity. He is a fellow of the American Academy of Arts and Sciences, the American Statistical Association, and the Institute of Physics.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Aerospace Village - Sunday - 10:00-13:59 PDT

Title: ARINC 664 CTF Challenge

Tags: Aerospace Village | Creator Event/Activity

When: Sunday, Aug 9, 10:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 2 700 (Aerospace Village) - [Map](#)

Description:

This is a two-part CTF activity designed to immerse participants in an aircraft's ARINC 664 network.

Virtual Challenge – Test your skills by navigating through a series of interactive tasks that build foundational knowledge of the ARINC 664 protocol – one of the communications protocols for onboard networks. Gain a high-level understanding of how this protocol operates and its security considerations.

Hardware Challenge: Take it to the next level by engaging with model hardware. Send messages to manipulate and interact with simulated aircraft systems!

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Aerospace Village - Friday - 10:00-17:59 PDT

Title: ARINC 664 CTF Challenge

Tags: Aerospace Village | Creator Event/Activity

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 2 700 (Aerospace Village) - [Map](#)

Description:

This is a two-part CTF activity designed to immerse participants in an aircraft's ARINC 664 network.

Virtual Challenge – Test your skills by navigating through a series of interactive tasks that build foundational knowledge of the ARINC 664 protocol – one of the communications protocols for onboard networks. Gain a high-level understanding of how this protocol operates and its security considerations.

Hardware Challenge: Take it to the next level by engaging with model hardware. Send messages to manipulate and interact with simulated aircraft systems!

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Aerospace Village - Saturday - 10:00-17:59 PDT

Title: ARINC 664 CTF Challenge

Tags: Aerospace Village | Creator Event/Activity

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 2 700 (Aerospace Village) - [Map](#)

Description:

This is a two-part CTF activity designed to immerse participants in an aircraft's ARINC 664 network.

Virtual Challenge – Test your skills by navigating through a series of interactive tasks that build foundational knowledge of the ARINC 664 protocol – one of the communications protocols for onboard networks. Gain a high-level understanding of how this protocol operates and its security considerations.

Hardware Challenge: Take it to the next level by engaging with model hardware. Send messages to manipulate and interact with simulated aircraft systems!

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Assume Breach, But For Real: Rewriting Infrastructure Policy for the Adversaries Who Never Left

Tags: Policy @ DEF CON | Creator Talk/Panel

When: Saturday, Aug 8, 15:30 - 15:59 PDT

Where: LVCCW Level 2 W210-211 (Policy Village) - [Map](#)

Description:

An energy provider detects an intrusion when a control-room operator notices an unexplained setpoint change not an alert. Initial access occurred ninety days earlier via a contractor credential that outlived contract. Disclosure clocks are already running. Scope is unknown. Systems cannot go offline. This reflects recurring patterns Microsoft incident response teams observe across critical infrastructure, patterns policy was not designed around today. Cyber policy assumes breaches are detectable in reasonable timeframes, attributable with confidence, and containable once identified. Incident response shows otherwise. PRC state-sponsored actors such as Volt Typhoon maintain persistent, low-visibility access using valid credentials and living-off-the-land techniques. Detection often lags weeks or months, triggered by operational impact rather than telemetry. Investigations unfold under live operations, incomplete visibility, and uncertain scope, while disclosure timelines under CIRCIA, SEC rules, NIS2, and similar frameworks continue to run. This session bridges incident response and policy design, drawing on CI cases, DOJ experience, crisis counsel to show where assumptions break and how policy can align to conditions: identity-driven intrusion, persistent access, IT-OT convergence, and decisions under uncertainty.

Speakers: Travis Berent, Adam Hickey

SpeakerBio: Travis Berent, Microsoft

Travis Berent is the Director of Security Business Strategy at Microsoft, where he helps shape the company's approach to incident response, resilience, and cybersecurity partnerships. Prior to joining Microsoft, Travis served as Director for Cybersecurity Policy and Incident Response at the National Security Council, where he strengthened U.S. defense and intelligence environments, oversaw response to significant cyber incidents affecting critical infrastructure and government networks, and led key processes including the Vulnerabilities Equities Process. He also helped develop national policy responses to ransomware and contributed to both the National Security Strategy and National Cyber Strategy. Earlier in his career, Travis served in multiple roles at the Federal Bureau of Investigation (FBI), including in the New York Field Office and at Cyber Division Headquarters, where he worked on counterintelligence and cyber matters.

SpeakerBio: Adam Hickey, Mayer Brown

Adam Hickey offers clients extensive experience in cybersecurity and national security matters. Adam draws on more than 15 years of experience at the U.S. Department of Justice (DOJ) handling high-profile national security matters intersecting with the private sector. Prior to joining Mayer Brown, he was a Deputy Assistant Attorney General (DAAG) of DOJ's National Security Division (NSD). During his time at NSD, Adam established DOJ's national security cyber program, dedicated to combatting malicious cyber activity by foreign intelligence services affecting major companies and critical infrastructure, and he supervised the criminal investigation and charging of every such case for more than a decade. He now advises critical infrastructure and OT operators on incident response, privileged investigations, disclosure, regulatory requirements across borders, and enforcement actions.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Social Gatherings/Events - Friday - 16:00-18:59 PDT

Title: Atlanta Metro Meetup (DC404/DC678/DC770/DC470)

Tags: Meetup

When: Friday, Aug 7, 16:00 - 18:59 PDT

Where: LVCCW Level 3 W327 (Misc Meeting Room) - [Map](#)

Description:

They say Atlanta is the city too busy to hate, but it also has too much traffic for its widespread hacker fam to get together in a single meetup. So instead, we're meeting up in the desert during DEF CON! The one time of year when intown, northern burbs, south siders, and anyone else connected to DC404's 30+ year legacy can catch up and share stories. Join us and meet your fellow ATL hackers!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Red Team Village - Sunday - 10:00-14:59 PDT

Title: Attack Campaign in VR

Tags: Red Team Village | Misc

When: Sunday, Aug 9, 10:00 - 14:59 PDT

Where: LVCCW Level 1 Hall 1 309 (Red Team Village) Special/Quest Area - [Map](#)

Description:

This VR visualization experience is designed to support the exploration and understanding of complex cybersecurity scenarios for students and professionals. Cyber attack campaigns often involve intricate relationships and multi-stage processes that can be difficult to interpret, making effective analysis and remediation challenging. By leveraging visualization best practices in virtual reality, the experience presents cyber threat information in a more intuitive and interactive format, with the goal of improving comprehension, situational awareness, and the ability to identify meaningful and actionable insights.

SpeakerBio: James Rice

Mr. James Rice has been cybersecurity faculty for the last decade in Upstate New York at Mohawk Valley Community College and more recently Rochester Institute of Technology. During this time, Mr. Rice has focused on developing numerous interactive gamified learning scenarios for the classroom and cyber competitions such as the NSA sponsored NCAE Cyber Games. Mr. Rice is currently pursuing his PhD at RIT in Computer Engineering and researching how to best leverage immersive reality technologies for data visualization and interaction, primarily in cyberspace.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Automated Discovery of Prompt Injection Vulnerabilities via Mutated Prompt Generation

Tags: Bug Bounty Village | Creator Talk/Panel

When: Sunday, Aug 9, 11:30 - 11:59 PDT

Where: LVCCW Level 1 Hall 3 1102 (Creator Stage 6) - [Map](#)

Description:

Finding one prompt injection isn't the end goal; checking how many variants still bypass your safeguarding layers is the new target. Introducing MPG, an XPIA mutation framework that generates adversarial payload variants and tests them across agentic AI systems to expose hidden vulnerability surfaces and emerging data exfiltration risks.

Speakers: Bogdan Steele, Arnav Garg

SpeakerBio: Bogdan Steele, Senior Software Engineer, Microsoft

Bogdan Stelea is a Senior Software Engineer performing AI Security Research at Microsoft, working at the intersection of AI security, adversarial ML, and secure agentic system design. Bogdan develops automated frameworks for conducting variant hunting and discovering prompt injection vulnerabilities at scale. His work focuses on identifying, reproducing, and understanding vulnerabilities in modern AI copilot solutions, with a particular emphasis on cross/indirect prompt injection attacks (XPIA), tool misuse, and the expanding attack surface introduced by AI agents. Moreover, Bogdan creates learning materials and courses that clearly explain the threats introduced by XPIA. Actively engaged in the AI Security, CTF, and Bug Bounty communities, with a consistent presence at DEF CON, Bogdan has published and presented his AI security research at international academic venues, including IEEE and ACM.

SpeakerBio: Arnav Garg, Security Researcher, Microsoft

Arnav Garg is a Security Researcher at the Microsoft Security Response Center (MSRC), specializing in AI security research, adversarial testing, and the security of Copilot and agentic AI systems. His work focuses on understanding and mitigating emerging AI threats, with particular emphasis on cross/indirect prompt injection attacks (XPIA), data exfiltration techniques, tool misuse, and the evolving attack surface introduced by AI agents. Arnav develops automated frameworks for scalable security testing and vulnerability discovery, helping advance practical defenses for next-generation AI systems. He has presented and published research on AI security, automated prompt injection discovery, and AI vulnerability testing at both internal and external venues.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Red Team Village - Friday - 14:00-15:59 PDT

Title: Automated Mythic Deployment with Gaia

Tags: Red Team Village | Misc

When: Friday, Aug 7, 14:00 - 15:59 PDT

Where: LVCCW Level 1 Hall 1 309 (Red Team Village) Tactic Table 3 - [Map](#)

Description:

Deploying a C2 server manually is a time consuming, sometimes annoying process. Deploying a C2 server weekly for two months, even more so. This Tactic will cover Gaia, the tool developed by the Midwest Collegiate Cyber Defense Competition Red Team to handle automated C2 deployment, user provisioning, payload creation, and more.

This Tactic will have attendees start with a standard Debian VM, and end with a fully provisioned Mythic server that can serve as the foundation for your next CTF, lab, or with a little extra work, your next op.

SpeakerBio: Shad Brown

Shad is an Associate Adversary Simulation Consultant at SpecterOps where he performs a variety of offensive security assessments. Prior to his time at SpecterOps, he had roles in vulnerability management and network security engineering.

He enjoys teaching and mentorship and has spoken to students and faculty at dozens of high schools, colleges, and universities across the United States. In the last few years, he has volunteered as the red team lead for the states of Minnesota and Indiana in the Collegiate Cyber Defense Competition.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Cloud Village - Saturday - 14:10-14:50 PDT

Title: Autonomous Offense vs. Autonomous Defense: Who's Winning in the Cloud?

Tags: Cloud Village | Creator Talk/Panel

When: Saturday, Aug 8, 14:10 - 14:50 PDT

Where: LVCCW Level 3 W313 (Cloud Village Talks) - [Map](#)

Description:



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Aerospace Village - Friday - 10:00-17:59 PDT

Title: Aviation ISAC Cybersecurity Challenge

Tags: Aerospace Village | Creator Event/Activity

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 2 700 (Aerospace Village) - [Map](#)

Description:

Chaos has ensued at a major international airport. Flight info displays flicker with false data. Baggage systems fail. Aircraft controls and drones (by the riverside) are compromised. Even the skies are no longer safe.

Your mission: investigate the breach, neutralize the threats, and take back control of the airport. The airport depends on you. The clock is ticking!

As a participant, your first step is to register ahead and read the rules at: <https://aviationcyberctf.com/> and bring your own laptop to the venue.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Aerospace Village - Saturday - 10:00-17:59 PDT

Title: Aviation ISAC Cybersecurity Challenge

Tags: Aerospace Village | Creator Event/Activity

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 2 700 (Aerospace Village) - [Map](#)

Description:

Chaos has ensued at a major international airport. Flight info displays flicker with false data. Baggage systems fail. Aircraft controls and drones (by the riverside) are compromised. Even the skies are no longer safe.

Your mission: investigate the breach, neutralize the threats, and take back control of the airport. The airport depends on you. The clock is ticking!

As a participant, your first step is to register ahead and read the rules at: <https://aviationcyberctf.com/> and bring your own laptop to the venue.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Aerospace Village - Sunday - 10:00-13:59 PDT

Title: Aviation ISAC Cybersecurity Challenge

Tags: Aerospace Village | Creator Event/Activity

When: Sunday, Aug 9, 10:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 2 700 (Aerospace Village) - [Map](#)

Description:

Chaos has ensued at a major international airport. Flight info displays flicker with false data. Baggage systems fail. Aircraft controls and drones (by the riverside) are compromised. Even the skies are no longer safe.

Your mission: investigate the breach, neutralize the threats, and take back control of the airport. The airport depends on you. The clock is ticking!

As a participant, your first step is to register ahead and read the rules at: <https://aviationcyberctf.com/> and bring your own laptop to the venue.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Contests - Friday - 10:00-12:59 PDT

Title: Aw, man...pages!

Tags: Aw, man...pages! | Contest

When: Friday, Aug 7, 10:00 - 12:59 PDT

Where: LVCCW Level 1 Hall 1 100 (Contest Stage) - [Map](#)

Description:

How well do you know your man pages? Find out by teaming up with up to 3 other people (or come solo and get matched up with some new friends) and play "Aw, man...pages!". Across several rounds, your knowledge of man pages and software will be tested to the limit. Can you remember what command line flag is being described by its help text? Can you identify a tool just from a man page snippet? Can you decipher our cryptic command clues? Will you prove yourself worthy to be crowned the man page champion?

Participant Prerequisites

None. We will provide answer sheets and pens. Participants can form teams of up to 4 people beforehand, or at the event.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: AzProwl: Prowling the Azure Attack Surface

Tags: DEF CON Demo Labs | Intermediate | Cloud | Defense/Blue Team | Offense/Red Team | Purple Team | DEF CON Demo Labs

When: Friday, Aug 7, 15:00 - 15:45 PDT

Where: LVCCW Level 1 Hall 3 900 (Demo Labs Track 4) - [Map](#)

Description:

Cloud environments aren't being breached through zero-days—they're being traversed through identity, misconfigurations, and overlooked data paths. Azure is no exception.

This talk introduces AzProwl, an offensive-focused tool designed to emulate how real attackers enumerate and chain together access across Azure environments. Rather than stopping at surface-level enumeration, AzProwl maps identity relationships, token abuse opportunities, and data plane exposure to uncover realistic attack paths.

We'll walk through how attackers move from initial access to meaningful impact using Azure-native mechanisms—leveraging identity roles, service principals, tokens, and storage access. Attendees will see how seemingly low-risk permissions compound into high-impact compromise.

Whether you're red team, blue team, or somewhere in between, this session will provide practical insight into how Azure environments are actually attacked—and how to detect and defend against it.

Speakers: Jared "GonePhishing402" Graff, Jeff Daniels

SpeakerBio: Jared "GonePhishing402" Graff

I'm a Lead Incident Response Analyst at Target with experience spanning red team operations, blue team defense, and incident response. My background working in Azure cloud security at Microsoft helped shape my approach to understanding and defending modern cloud environments and ultimately inspired the development of this training.

I specialize in analyzing and emulating real-world attack paths across cloud identities, authentication tokens, and data planes to uncover gaps in detection and response capabilities. My work focuses on Azure identity compromise, token abuse, cloud persistence techniques, and understanding how adversaries actually operate within cloud environments—not just how we assume they do.

I'm passionate about bridging the gap between offensive and defensive security, translating attacker tradecraft into actionable detection strategies, and developing hands-on labs that help defenders better understand cloud threats. My goal is to make complex attack techniques accessible, practical, and directly applicable to real-world security operations.

SpeakerBio: Jeff Daniels

Jeff Daniels is a Senior Cloud Solution Architect at Microsoft Federal specializing in cloud security, threat intelligence, and red team operations. With a background in military cyber operations, he brings real-world offensive experience to designing detection strategies, Zero Trust architectures, and large-scale SOC capabilities. Jeff focuses on translating adversary tradecraft into actionable security outcomes for government customers and is actively involved in red team tooling, adversary emulation, and ATT&CK-aligned training.

Title: AzProwl: Prowling the Azure Attack Surface

Tags: DEF CON Demo Labs | Intermediate | Cloud | Defense/Blue Team | Offense/Red Team | Purple Team | DEF CON Demo Labs

When: Friday, Aug 7, 14:00 - 14:45 PDT

Where: LVCCW Level 1 Hall 3 900 (Demo Labs Track 4) - [Map](#)

Description:

Cloud environments aren't being breached through zero-days—they're being traversed through identity, misconfigurations, and overlooked data paths. Azure is no exception.

This talk introduces AzProwl, an offensive-focused tool designed to emulate how real attackers enumerate and chain together access across Azure environments. Rather than stopping at surface-level enumeration, AzProwl maps identity relationships, token abuse opportunities, and data plane exposure to uncover realistic attack paths.

We'll walk through how attackers move from initial access to meaningful impact using Azure-native mechanisms—leveraging identity roles, service principals, tokens, and storage access. Attendees will see how seemingly low-risk permissions compound into high-impact compromise.

Whether you're red team, blue team, or somewhere in between, this session will provide practical insight into how Azure environments are actually attacked—and how to detect and defend against it.

Speakers: Jared "GonePhishing402" Graff, Jeff Daniels

SpeakerBio: Jared "GonePhishing402" Graff

I'm a Lead Incident Response Analyst at Target with experience spanning red team operations, blue team defense, and incident response. My background working in Azure cloud security at Microsoft helped shape my approach to understanding and defending modern cloud environments and ultimately inspired the development of this training.

I specialize in analyzing and emulating real-world attack paths across cloud identities, authentication tokens, and data planes to uncover gaps in detection and response capabilities. My work focuses on Azure identity compromise, token abuse, cloud persistence techniques, and understanding how adversaries actually operate within cloud environments—not just how we assume they do.

I'm passionate about bridging the gap between offensive and defensive security, translating attacker tradecraft into actionable detection strategies, and developing hands-on labs that help defenders better understand cloud threats. My goal is to make complex attack techniques accessible, practical, and directly applicable to real-world security operations.

SpeakerBio: Jeff Daniels

Jeff Daniels is a Senior Cloud Solution Architect at Microsoft Federal specializing in cloud security, threat intelligence, and red team operations. With a background in military cyber operations, he brings real-world offensive experience to designing detection strategies, Zero Trust architectures, and large-scale SOC capabilities. Jeff focuses on translating adversary tradecraft into actionable security outcomes for government customers and is actively involved in red team tooling, adversary emulation, and ATT&CK-aligned training.

The Diana Initiative - Saturday - 13:50-13:59 PDT

Title: Badgeline Tour

Tags: The Diana Initiative | Creator Tour

When: Saturday, Aug 8, 13:50 - 13:59 PDT

Where: LVCCW Level 1 South Lobby / Atrium - [Map](#)

Description:

Interested in visiting Badgeline but afraid to go by yourself? The Diana Initiative is hosting tours! Follow a volunteer to Badgeline and be introduced to the community and activities inside!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: BadVR: Signals Everywhere a collaboration with XR Village

Tags: OWASP Foundation | Creator Event/Activity

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 4 1415 (OWASP Foundation) - [Map](#)

Description:

BadVR Data Exploration through VR visualization. See RF signals, cellular signals and new for 2026, Meshtastic signals, step into the data with a hands-on VR experience

Speakers: Jad Meouchy, Suzanne Borders

SpeakerBio: Jad Meouchy, CTO + Co-Founder at BadVR

Jad, originally from northern Virginia, holds dual B.S. degrees in Computer Engineering and Psychology from Virginia Tech, and is a graduate of the Thomas Jefferson High School for Science and Technology. While in college, he engineered and built the data visualization components of an emergency response simulation that went on to receive 2M in public grant funding. Over his 15-year career, Jad has founded five startups and successfully exited three. His professional expertise is in software architecture and development, specifically big data analytics and visualization, and virtual and augmented reality development. Based in Los Angeles since 2010, Jad promotes the community by organizing developer meetups and events, and volunteering time for STEM initiatives.

SpeakerBio: Suzanne Borders, CEO + Founder at BadVR

Suzanne studied psychology at University of Missouri, Kansas City and previously worked as Lead UX/Product Designer for over 9 years at companies such as Remine (raised \$48M) and CREXi (raised \$54M) where she specialized in designing intuitive, high-performant data analytic interfaces. In 2019, Suzanne founded BadVR and was awarded a “Rising Stars” innovation award from IEEE. To date, she’s raised over \$4M in non-dilutive funding for BadVR, via grants from the National Science Foundation, NOAA, Magic Leap, Qualcomm, and more. Suzanne has grown the company from 2 to 25 people and was awarded 4 patents for innovations she created while leading the BadVR team. Over the past 5 years, Suzanne emerged as a thought-leader in the immersive data visualization and analytics space. She has been a keynote speaker at over 25 national and international conferences. In her spare time, Suzanne travels for inspiration (81 countries and counting) and is proud to be a published author and former punk. Suzanne thrives at the intersection of product design, immersive technology, and data; she’s a believer in the artistry of technology and the technicality of art and remains passionately dedicated to democratizing access to data through universally accessible products.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: BadVR: Signals Everywhere a collaboration with XR Village

Tags: OWASP Foundation | Creator Event/Activity

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 4 1415 (OWASP Foundation) - [Map](#)

Description:

BadVR Data Exploration through VR visualization. See RF signals, cellular signals and new for 2026, Meshtastic signals, step into the data with a hands-on VR experience

Speakers: Jad Meouchy, Suzanne Borders

SpeakerBio: Jad Meouchy, CTO + Co-Founder at BadVR

Jad, originally from northern Virginia, holds dual B.S. degrees in Computer Engineering and Psychology from Virginia Tech, and is a graduate of the Thomas Jefferson High School for Science and Technology. While in college, he engineered and built the data visualization components of an emergency response simulation that went on to receive 2M in public grant funding. Over his 15-year career, Jad has founded five startups and successfully exited three. His professional expertise is in software architecture and development, specifically big data analytics and visualization, and virtual and augmented reality development. Based in Los Angeles since 2010, Jad promotes the community by organizing developer meetups and events, and volunteering time for STEM initiatives.

SpeakerBio: Suzanne Borders, CEO + Founder at BadVR

Suzanne studied psychology at University of Missouri, Kansas City and previously worked as Lead UX/Product Designer for over 9 years at companies such as Remine (raised \$48M) and CREXi (raised \$54M) where she specialized in designing intuitive, high-performant data analytic interfaces. In 2019, Suzanne founded BadVR and was awarded a “Rising Stars” innovation award from IEEE. To date, she’s raised over \$4M in non-dilutive funding for BadVR, via grants from the National Science Foundation, NOAA, Magic Leap, Qualcomm, and more. Suzanne has grown the company from 2 to 25 people and was awarded 4 patents for innovations she created while leading the BadVR team. Over the past 5 years, Suzanne emerged as a thought-leader in the immersive data visualization and analytics space. She has been a keynote speaker at over 25 national and international conferences. In her spare time, Suzanne travels for inspiration (81 countries and counting) and is proud to be a published author and former punk. Suzanne thrives at the intersection of product design, immersive technology, and data; she’s a believer in the artistry of technology and the technicality of art and remains passionately dedicated to democratizing access to data through universally accessible products.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Bait the Bot: Hacking Back Autonomous AI Vulnerability Scanners

Tags: La Villa Community | Creator Talk/Panel

When: Sunday, Aug 9, 10:30 - 11:30 PDT

Where: LVCCW Level 1 Hall 4 1416 (La Villa Community) Main Stage - [Map](#)

Description:

Autonomous, LLM-powered vulnerability scanners now crawl the web at scale — and every one of them shares the same structural weakness: it reads the content you control. This talk flips the engagement. Instead of just blocking the bot, your site detects that an AI agent is scanning it, fingerprints the model behind it, and fires back a hidden, tailored prompt injection that derails, poisons, or neutralizes the attacking agent — with no traditional exploit involved. We build on recent academic work on prompt-injection "hack back," push it into the reconnaissance-and-scanning threat model with live demos, walk through an escalating cat-and-mouse between attacker and defender, and take an honest look at where active defense crosses the legal line. Red teamers and blue teamers alike will leave with something they can responsibly test the same week.

SpeakerBio: Alcyon Junior, Head of Offensive Security & Fraud Hunting at Apura

Alcyon Junior is the Head of Offensive Security & Fraud Hunting at Apura, a speaker, writer, EXIN-accredited instructor, SecurityCast (securitycast.com.br) podcaster, and professor. He holds three degrees in Information Technology with a focus on computer networks, is a Cisco-certified specialist in Computer Networks, and has an MBA in IT Governance. Alcyon earned a Master's degree in Knowledge Management and Information Technology with a focus on Cybersecurity from the Catholic University of Brasília, and he is currently pursuing a PhD in Electrical Engineering with an emphasis on Information Security and Communications at the University of Brasília (UnB). His international certifications include CompTIA Security+, Ethical Hacking Foundation (EHF), ISO/IEC 27002 (ISFS), ITIL® Foundation, Cisco Networking Academy (CNAP), McAfee Vulnerability Manager (MVM), and Server Professional (LPIC-1)

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Bashing CloudShells for mining, networking, exfil and persistence at scale

Tags: Cloud Village | Creator Talk/Panel

When: Saturday, Aug 8, 10:00 - 10:40 PDT

Where: LVCCW Level 3 W313 (Cloud Village Talks) - [Map](#)

Description:

CloudBashing started with reversing the private AWS, Azure, and GCP CloudShell REST protocols, analyzing websocket terminal sessions, and tracing janky browser authentication/credential flows with cookies and OAuth tokens. Along the way, we automated the APIs to access free CPU/networking, maintained access across container/VM resets, utilized persistent \$HOME for implants/data, locked users out of sudo access, and installed a C2 framework. We discovered IAM design issues like: AWS role assumption that result in a large # of environments per compromised identity, web socket sessions that survive API token revocation, and M365/Gmail consumer email accounts that have default CloudShell access. This turned into a newly released exploit toolkit, CloudBasher, that enumerates, validates, installs, and runs distributed workloads with virtual storage and private networking across a large-scale agent network with persistence and resilience. We'll demo distributing CPU-intensive workloads, using virtual storage for staging/exfiltration, secure networking for proxy and obfuscated exfil paths, while automating the discovery, enumeration, creation of CloudShell environments from initial credentials/sessions to implants/setup/networking to management and control.

Speakers: Jenko "edleft" Hwong, Chris Ryan

SpeakerBio: Jenko "edleft" Hwong, Huntress Labs

Jenko Hwong is a Principal Security Researcher at Huntress Labs, focusing on identity-based attacks and cloud abuse. Prior to Huntress, he spent 6 years at Netskope Threat Labs, has spoken at RSA and DEFCON, and is a Cloud Village Lead. He has over 20 years at various security startups in cloud detection/response, vulnerability scanning, AV/AS, pen-testing/exploits, L3/4 appliances, threat intel, and windows security.

SpeakerBio: Chris Ryan, Huntress Labs

A series of oddly configured server banners, a JARM fingerprint, curious fields in a security certificate - these aren't just technical details, but are instead threads in a narrative tapestry woven like a John le Carre novel. For over 20 years, Chris has dedicated his life to studying these threads and the intersection between cybersecurity, Russian linguistics, and free and open source software. His career path has taken detours through academia, aerospace and defense, software development, and cybersecurity.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Social Engineering Community Village - Saturday - 10:15-13:15 PDT

Title: Battle of the Bots: Vishing Edition

Tags: Social Engineering Community Village | Creator Event/Activity

When: Saturday, Aug 8, 10:15 - 13:15 PDT

Where: LVCCW Level 3 W317-319 (Social Engineering Community Village) - [Map](#)

Description:

AI meets vishing in the booth as teams use AI-powered agents to place live calls, chase preset objectives, and test the limits of automation, hacking, and human psychology. Judged by Snow, Perry Carpenter, and Lisa Flynn.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: BBOT: Automating the OSINT Kill Chain with a Single Command

Tags: Recon Village | Creator Workshop

When: Friday, Aug 7, 15:30 - 17:59 PDT

Where: LVCCW Level 1 Hall 2 501 (Recon Village) - [Map](#)

Description:

Reconnaissance is the foundation of every successful engagement but fragmented tooling, manual chaining, and missed data leave gaps that cost you findings. BBOT (Bighuge BLS OSINT Tool) was built to solve that. Developed by Black Lantern Security, BBOT is a recursive, event-driven OSINT framework that replaces the traditional phased approach with continuous, real-time discovery every new piece of data is immediately fed back into the scan engine to uncover what linear workflows miss.

This is a fully hands-on workshop. Attendees will install and configure BBOT, then run it live against their own scoped bug bounty targets turning the session into real reconnaissance rather than a slide-driven demo. We'll cover BBOT's 100+ module architecture spanning subdomain enumeration, cloud asset discovery, email harvesting, web spidering, and vulnerability scanning with Nuclei, all chainable in a single command and firing recursively in real time. Along the way we'll dig into scope management, passive vs. active recon tradeoffs, and the web hacking modules that can point you toward real findings.

By the end of the session, attendees will walk away with actual scan output from a live target, a repeatable BBOT-driven recon workflow they can drop into their next program, and a clear understanding of how to triage findings into real submissions. Whether you're new to automated recon or a seasoned bug bounty hunter still stitching tools together by hand, this workshop will change how you approach OSINT at scale.

Module 1 — Why BBOT? The Problem with How We Recon Now

The fragmented toolchain problem: Amass Subfinder httpx manual grep

Why phased OSINT misses things — and what recursive, event-driven recon solves

BBOT's origin at Black Lantern Security and design philosophy

Quick architecture overview: modules, events, presets, scope

3.0 Updates - Rustification of HTTP and DNS

Q&A / audience skill check

Module 2 — Getting Oriented: Installation, Config & First Scan

Verify install and run `bbot --help`

Listing and exploring modules with `bbot -l`

Understanding flags vs. modules vs. presets

Exercise 2.1: Run your first subdomain scan

Reading and understanding BBOT output

Scan output folders, naming conventions, and where data lives

Module 3 — Subdomain Enumeration Deep Dive

How BBOT's recursive engine finds more than traditional tools

Passive vs. active enumeration — when to use each

Subdomain mutations and wordcloud usage

Exercise 3.1: Full active subdomain enum

Module 4 — Going Deeper: Cloud, Email & Asset Discovery

Cloud enumeration: S3 buckets, Azure blobs, GCP assets

Email harvesting for org footprinting

Combining flags for broader discovery

Exercise 4.1: Run a combined cloud + email + subdomain scan

Identifying misconfigured or exposed cloud assets in output

Discussion: how these findings translate to bug bounty submissions

Module 5 — Web Hacking Modules & Vulnerability Scanning

Overview of BBOT's web module suite: httpx, gowitness, wappalyzer, nuclei

Web spidering for email, secrets, and exposed paths

Nuclei integration — what it scans for and how to interpret results

Exercise 5.1: Full web scan with screenshots

Exercise 5.2: Kitchen sink scan (instructor-guided, safe target only)

Setting expectations: BBOT points you at the doors — you still have to kick them open

Module 6 — Triage, Workflow & What Happens After the Scan

How to structure your post-BBOT workflow: what to investigate first

Prioritizing findings by severity and exploitability

Avoiding common pitfalls: rate limiting, duplicate findings, out-of-scope mistakes

Building a repeatable bug bounty recon workflow around BBOT

Scheduling and automating recurring scans for continuous monitoring

Wrap-Up & Q&A

Recap of key takeaways

Recommended next steps and resources

[GitHub](#), [docs](#), and [community links](#)

[Open Q&A](#)

SpeakerBio: Mark Gaddy

No BIO available

[Return to Index](#) - [Add to Google](#)



- ics [Calendar](#) file

The Diana Initiative - Saturday - 12:30-12:40 PDT

Title: BBWIC Foundation Tour

Tags: The Diana Initiative | Creator Tour

When: Saturday, Aug 8, 12:30 - 12:40 PDT

Where: LVCCW Level 1 South Lobby / Atrium - [Map](#)

Description:

Interested in visiting BBWIC Foundation but afraid to go by yourself? The Diana Initiative is hosting tours! Follow a volunteer to BBWIC Foundation and be introduced to the community and activities inside!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Be like a BRAT(BLE Recon and Attack Toolkit): Skip the Handshake, Own the Device

Tags: Intro/Beginner | DEF CON Demo Labs | AppSec | Hardware/IoT | Mobile | Offense/Red Team | Wireless/RF | DEF CON Demo Labs

When: Saturday, Aug 8, 15:00 - 15:45 PDT

Where: LVCCW Level 1 Hall 3 1003 (Demo Labs Track 3) - [Map](#)

Description:

What happens when you buy a popular medical device and realize it blindly trusts any BLE connection within 30 meters?

BRAT (BLE Recon and Attack Toolkit) is the open-source Python arsenal we built to systematically take over an FDA-listed consumer hormone analyzer and generalize the attack to the class of devices behind it. Relying on the Nordic UART Service (NUS), the target blindly trusts any connection within 30 meters. BRAT automates the exact attack chain we used to compromise it: passive BLE discovery, protocol reverse engineering, unauthenticated command injection, full bind takeover, and rogue peripheral impersonation to hijack live API session tokens.

Every script is built on the †bleak† async BLE library and deliberately kept small so you can read the code and understand the exploit in minutes. Our Demo Lab features live, end-to-end attacks against a consumer medical device. We'll demonstrate unauthenticated command injection, rogue peripheral spoofing that intercepts companion app handshakes, and how we injected spoofed hormone sensor data without ever pairing.

Speakers:Gigi Xiaoqing Liu,Muzzammil Mohammed,Narmina Karimova

SpeakerBio: Gigi Xiaoqing Liu

Gigi Liu is a graduate security researcher at Northeastern's Security And Privacy Research (SPQR) Group under Professor Kevin Fu, where her work covers embedded systems security, medical device attack surfaces, and AI-generated media detection. She interns at Lila Sciences as a Security and Cloud Engineer, building enterprise-wide agentic AI security infrastructure and detection capabilities for unauthorized AI activity across cloud and SaaS environments.

Her technical work spans wireless protocol reverse engineering, binary exploitation, web and mobile reverse engineering, cloud and AI security. She has applied these skills across medical hardware, automotive platforms, and enterprise cloud environments — from BLE command injection on FDA-listed devices to CarPlay API exploitation to building agentic AI detection controls at scale. As a UCLA psychobiology alum with a consulting background, she brings a multidisciplinary lens to every system: understand what it's designed to do first, then find where it breaks.

SpeakerBio: Muzzammil Mohammed

Muzzammil Mohammed is an offensive security researcher, penetration tester at Maltek Solutions, and MS in Cybersecurity at Northeastern University. Operating out of the SPQR Lab under Professor Kevin Fu, and serving as a Teaching Assistant Network Security, his work bridges academic vulnerability research with real-world red team execution. As a core developer of WandKit an open-source BLE attack toolkit built to audit medical devices. Muzzammil led the cloud API exploitation phase, successfully confirming a complete authentication bypass and engineering the rogue peripheral session hijack chain. Beyond hardware and API hacking, he is actively developing autonomous multi-agent AI frameworks designed to orchestrate local LLMs for automated security auditing and vulnerability analysis.

SpeakerBio: Narmina Karimova

Narmina Karimova is a cybersecurity graduate researcher at Northeastern University with a background in enterprise technology across financial institutions and the United Nations. She came to security research from the infrastructure side,

which shaped how she approached tearing apart a consumer fertility monitor. For BRAT, she wrote the core BLE attack suite in Python: replay modules, rogue peripheral session capture, unauthenticated hormone data extraction, and the bind takeover chain that captures device ownership in under 15 seconds. She also reverse-engineered the APK with JADX, found hardcoded credentials, and confirmed a CVSS 9.1 IDOR in the third-party integration. Her interest is in the gap between how consumer health devices are marketed and how they actually handle sensitive data.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Be like a BRAT(BLE Recon and Attack Toolkit): Skip the Handshake, Own the Device

Tags: Intro/Beginner | DEF CON Demo Labs | AppSec | Hardware/IoT | Mobile | Offense/Red Team | Wireless/RF | DEF CON Demo Labs

When: Friday, Aug 7, 11:00 - 11:45 PDT

Where: LVCCW Level 1 Hall 3 1003 (Demo Labs Track 3) - [Map](#)

Description:

What happens when you buy a popular medical device and realize it blindly trusts any BLE connection within 30 meters?

BRAT (BLE Recon and Attack Toolkit) is the open-source Python arsenal we built to systematically take over an FDA-listed consumer hormone analyzer and generalize the attack to the class of devices behind it. Relying on the Nordic UART Service (NUS), the target blindly trusts any connection within 30 meters. BRAT automates the exact attack chain we used to compromise it: passive BLE discovery, protocol reverse engineering, unauthenticated command injection, full bind takeover, and rogue peripheral impersonation to hijack live API session tokens.

Every script is built on the †bleak† async BLE library and deliberately kept small so you can read the code and understand the exploit in minutes. Our Demo Lab features live, end-to-end attacks against a consumer medical device. We'll demonstrate unauthenticated command injection, rogue peripheral spoofing that intercepts companion app handshakes, and how we injected spoofed hormone sensor data without ever pairing.

Speakers:Gigi Xiaoqing Liu,Muzzammil Mohammed,Narmina Karimova

SpeakerBio: Gigi Xiaoqing Liu

Gigi Liu is a graduate security researcher at Northeastern's Security And Privacy Research (SPQR) Group under Professor Kevin Fu, where her work covers embedded systems security, medical device attack surfaces, and AI-generated media detection. She interns at Lila Sciences as a Security and Cloud Engineer, building enterprise-wide agentic AI security infrastructure and detection capabilities for unauthorized AI activity across cloud and SaaS environments.

Her technical work spans wireless protocol reverse engineering, binary exploitation, web and mobile reverse engineering, cloud and AI security. She has applied these skills across medical hardware, automotive platforms, and enterprise cloud environments — from BLE command injection on FDA-listed devices to CarPlay API exploitation to building agentic AI detection controls at scale. As a UCLA psychobiology alum with a consulting background, she brings a multidisciplinary lens to every system: understand what it's designed to do first, then find where it breaks.

SpeakerBio: Muzzammil Mohammed

Muzzammil Mohammed is an offensive security researcher, penetration tester at Maltek Solutions, and MS in Cybersecurity at Northeastern University. Operating out of the SPQR Lab under Professor Kevin Fu, and serving as a Teaching Assistant Network Security, his work bridges academic vulnerability research with real-world red team execution. As a core developer of WandKit an open-source BLE attack toolkit built to audit medical devices. Muzzammil led the cloud API exploitation phase, successfully confirming a complete authentication bypass and engineering the rogue peripheral session hijack chain. Beyond hardware and API hacking, he is actively developing autonomous multi-agent AI frameworks designed to orchestrate local LLMs for automated security auditing and vulnerability analysis.

SpeakerBio: Narmina Karimova

Narmina Karimova is a cybersecurity graduate researcher at Northeastern University with a background in enterprise technology across financial institutions and the United Nations. She came to security research from the infrastructure side,

which shaped how she approached tearing apart a consumer fertility monitor. For BRAT, she wrote the core BLE attack suite in Python: replay modules, rogue peripheral session capture, unauthenticated hormone data extraction, and the bind takeover chain that captures device ownership in under 15 seconds. She also reverse-engineered the APK with JADX, found hardcoded credentials, and confirmed a CVSS 9.1 IDOR in the third-party integration. Her interest is in the gap between how consumer health devices are marketed and how they actually handle sensitive data.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Noob Community - Sunday - 12:30-12:59 PDT

Title: Be your own Agent: Career Journey and Advice from IT and STEM Educator to Cybersecurity Engineer

Tags: Noob Community | Creator Talk/Panel

When: Sunday, Aug 9, 12:30 - 12:59 PDT

Where: LVCCW Level 1 Hall 4 1417 (Noob Community) - [Map](#)

Description:

A career journey may have many twists and turns - mine certainly has! This talk will explore some themes from my pivot to cybersecurity and my journey through threat intelligence, a offensive security startup, and a Federally Funded Research and Development Center (FFRDC). We'll explore ways to advocate for yourself, suggestions for pivots and early career choices, and wrap it all up with thoughts on what can be next. Parts of the talk will be interactive and questions are encouraged.

So, what do you want to be and how can agency and being your own agent help you in your career journey?

SpeakerBio: Meghan Jacquot

No BIO available

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: beacon injected with HOOKCHAIN 2026

Tags: Red Team Village | Misc

When: Sunday, Aug 9, 14:00 - 14:59 PDT

Where: LVCCW Level 1 Hall 1 309 (Red Team Village) Tactic Table 3 - [Map](#)

Description:

In penetration testing, we constantly find ourselves facing EDRs/AVs, etc. But as in all cases, we aim to develop our own tooling or techniques that we believe may not yet be properly mapped or detected. On this occasion, we share part of our perspective when dealing with EDRs using Machine Learning technology configured in “FULL” mode. We were able to leverage this technique combined with an encrypted payload to evade this configuration; additionally, when the payload was downloaded or shared as a “.zip,” the agent did not inspect it. Now, let’s dive a bit into the technical aspects, but especially into how it was exploited. HookChain is an advanced technique for evading EDR solutions. It is primarily used by threat actors (APTs), but it can also be applied ethically in Red Team exercises. Its main principle is to intercept the hooks that EDRs install in the operating system kernel. What is a hook? Hooks are a mechanism used by EDRs to monitor calls to Windows API functions, mainly from ntdll.dll. In this way, they can intercept and analyze suspicious behavior in real time. The HookChain technique aims to bypass this monitoring layer.

Encrypting our payload with XOR HookChain typically combines hook evasion with payload encryption; in this case, we will use XOR to avoid static signature-based detection. The shellcode is encrypted in memory and only decrypted right before execution.

We can use a string (in this case, “CHANGEMYKEY”) as the key for our XOR encryption, along with shellcode generated using msfvenom, although we can also leverage other C2 frameworks, as we will see later.

SpeakerBio: Arnold Jared Morales Yopez, Senior Team Lead, Grupo Salinas

Self-taught in computer security since age 12; holds a degree in Computer Forensics and Cybersecurity and is pursuing a Master's in AI and Cybersecurity.

--

Desde los 12 años, me he dedicado a la informática con un enfoque especial en la seguridad. Actualmente, a mis 22 años, sigo explorando este mundo con la misma pasión, impulsado por la constante evolución de la tecnología y su interminable curva de aprendizaje.

Cuento con una carrera en Cómputo Forense y Ciberseguridad, actualmente curso una maestría en Inteligencia Artificial y Ciberseguridad.

Certificaciones: CWEE | CAPE | CPTS | EWPTX | CRT0 | eMAPT | OSCP | OSCP+ | CEH V13 | EJPT | HTB prolabs Hades - Cybernetics - Zephyr - APTlabs | MDK



[Return to Index](#) - Add to Google - ics [Calendar](#) file

DEF CON Training - Friday - 08:30-17:30 PDT

Title: Beat the Breach: Defend, Respond, Survive

Tags: DEF CON Training (Paid) (1-day) | DEF CON Training

When: Friday, Aug 7, 08:30 - 17:30 PDT

Where: LVCCW Level 2 W221 (Training) - [Map](#)

Description:

Speakers: McKay Hardy, Wes Wagstaff

SpeakerBio: McKay Hardy

No BIO available

SpeakerBio: Wes Wagstaff

No BIO available

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Beer Chilling Contraption Contest

Tags: Beer Chilling Contraption Contest | Contest

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 202 (Beer Chilling Contraption Contest) - [Map](#)

Description:

It's the 21st year of the BCCC and it's the Beer Chilling Contraption Contest this year! We can finally drink! No more beverage, we are drinking beer now, and boy do we need one. This year we thought we would mix it up and have cold beer and you all could try your hand at warming it. Unfortunately, the guys in charge of getting the ice got a bit too tan walking in this Vegas sun. A different kind of ICE deported them to Botswana and in the ensuing chaos the beverage was left outside and its warm again. Fortunately for everyone involved, WW3 and the inevitable nuclear winter will finally solve the warm beer problem -- well at least temperature-wise. It might be a little HOT in the gamma spectrum. But while we wait for Pooh Bear, BiBi, Putler, and or the Cheeto to kick this global cooling contraption off, its up to us to chill this beer.

You will cool the beer we give you in a red solo cup as quickly as possible to 34 degrees F. You may not alter the beer by mixing it with ice, dry or otherwise. You may bring a device you created or build your own at the convention. There are some great prizes waiting, mostly what I have lying around and don't want to take home. There are some additional rules, check the DEFCON forums or the poster board at the contest!

In conclusion, it's not just a warm beverage—it's a testament to the rich tapestry of societal collapse, seamlessly navigating the multifaceted landscape of your broken contraption.

Participant Prerequisites

- A commitment to the sanctity of the unadulterated beverage.
- A complete disregard for the health a safety of one's self, good design principals, and the laws of physics generally.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Beer Chilling Contraption Contest

Tags: Beer Chilling Contraption Contest | Contest

When: Sunday, Aug 9, 10:00 - 11:59 PDT

Where: LVCCW Level 1 Hall 1 202 (Beer Chilling Contraption Contest) - [Map](#)

Description:

It's the 21st year of the BCCC and it's the Beer Chilling Contraption Contest this year! We can finally drink! No more beverage, we are drinking beer now, and boy do we need one. This year we thought we would mix it up and have cold beer and you all could try your hand at warming it. Unfortunately, the guys in charge of getting the ice got a bit too tan walking in this Vegas sun. A different kind of ICE deported them to Botswana and in the ensuing chaos the beverage was left outside and its warm again. Fortunately for everyone involved, WW3 and the inevitable nuclear winter will finally solve the warm beer problem -- well at least temperature-wise. It might be a little HOT in the gamma spectrum. But while we wait for Pooh Bear, BiBi, Putler, and or the Cheeto to kick this global cooling contraption off, its up to us to chill this beer.

You will cool the beer we give you in a red solo cup as quickly as possible to 34 degrees F. You may not alter the beer by mixing it with ice, dry or otherwise. You may bring a device you created or build your own at the convention. There are some great prizes waiting, mostly what I have lying around and don't want to take home. There are some additional rules, check the DEFCON forums or the poster board at the contest!

In conclusion, it's not just a warm beverage—it's a testament to the rich tapestry of societal collapse, seamlessly navigating the multifaceted landscape of your broken contraption.

Participant Prerequisites

- A commitment to the sanctity of the unadulterated beverage.
- A complete disregard for the health a safety of one's self, good design principals, and the laws of physics generally.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Beer Chilling Contraption Contest

Tags: Beer Chilling Contraption Contest | Contest

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 202 (Beer Chilling Contraption Contest) - [Map](#)

Description:

It's the 21st year of the BCCC and it's the Beer Chilling Contraption Contest this year! We can finally drink! No more beverage, we are drinking beer now, and boy do we need one. This year we thought we would mix it up and have cold beer and you all could try your hand at warming it. Unfortunately, the guys in charge of getting the ice got a bit too tan walking in this Vegas sun. A different kind of ICE deported them to Botswana and in the ensuing chaos the beverage was left outside and its warm again. Fortunately for everyone involved, WW3 and the inevitable nuclear winter will finally solve the warm beer problem -- well at least temperature-wise. It might be a little HOT in the gamma spectrum. But while we wait for Pooh Bear, BiBi, Putler, and or the Cheeto to kick this global cooling contraption off, its up to us to chill this beer.

You will cool the beer we give you in a red solo cup as quickly as possible to 34 degrees F. You may not alter the beer by mixing it with ice, dry or otherwise. You may bring a device you created or build your own at the convention. There are some great prizes waiting, mostly what I have lying around and don't want to take home. There are some additional rules, check the DEFCON forums or the poster board at the contest!

In conclusion, it's not just a warm beverage—it's a testament to the rich tapestry of societal collapse, seamlessly navigating the multifaceted landscape of your broken contraption.

Participant Prerequisites

- A commitment to the sanctity of the unadulterated beverage.
- A complete disregard for the health a safety of one's self, good design principals, and the laws of physics generally.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Beerus Framework – A New Mobile Framework Arises

Tags: Mobile Hacking Community | Creator Talk/Panel

When: Saturday, Aug 8, 15:00 - 15:59 PDT

Where: LVCCW Level 1 Hall 4 1422 (Mobile Hacking Community) - [Map](#)

Description:

About a year ago, Hakai Security introduced the Beerus Framework, a proposal to unify mobile tools in order to streamline the penetration testing process directly on Android devices. The idea was simple: centralize tooling and optimize the testing environment setup, removing the need for complex configurations and reducing operational friction during assessments.

Today, after a year of evolution, the framework is no longer just a concept. It has become a robust platform for offensive mobile analysis, gaining international recognition within the community. In this talk, we revisit Beerus in its current form, exploring its evolution, the capabilities that have been consolidated over time, and the lessons learned from real-world scenarios.

We also discuss the future vision of the project, covering new features, technical challenges faced during its development, and how the framework can continue evolving to keep up with modern mobile security assessment demands.

Official blog post: <https://hakaioffsec.io/beerus-framework-a-new-mobile-framework-arises/insights-blog/> Repository:

<https://github.com/hakaioffsec/beerus-android> Community references: - mobile hacker (post):

<https://x.com/androidmalware2/status/1979100030884618375> - mobile hacker (video):

https://www.youtube.com/watch?v=8bDQzqw0_Sc - ZeroDay Gym (video):

<https://www.youtube.com/watch?v=I81xuVDsytE>

Speakers: João Pedro Tricta, Daniel "Daniboy" França Lima

SpeakerBio: João Pedro Tricta, Client-Side Applications Squad Leader, Researcher, and Malware Developer at Hakai Offensive Security

Known as Tricta, I am 20 years old, Brazilian, and work as a Client-Side Applications Squad Leader, Researcher, and Malware Developer at Hakai Offensive Security. I am passionate about Sysinternals, reverse engineering, low-level, and client-side applications. In my free time, I enjoy programming, gaming, and watching anime. I'm a cat lover and a compulsive pizza eater.

SpeakerBio: Daniel "Daniboy" França Lima, Pentester / Researcher at Hakai Offensive Security

Known as Daniboy, I am 19 years old, Brazilian, and work as a Pentester and Researcher at Hakai Offensive Security. I am passionate about understanding how things work, building tools, and manipulating systems. In my free time, I enjoy gaming, especially titles like Hollow Knight. I also love foxes, they are just too cute :3

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Aerospace Village - Saturday - 17:00-17:30 PDT

Title: Behind the Badge: SAOV3 and Open Sourcing the Aerospace Village ISS Badge

Tags: Aerospace Village | Creator Talk/Panel

When: Saturday, Aug 8, 17:00 - 17:30 PDT

Where: LVCCW Level 1 Hall 3 1103 (Creator Stage 5) - [Map](#)

Description:

The Rare Circuits team decided this was the year to take all our hard work on last year's Aerospace Village badge and open source the useful components for the Badge Maker Community. We took the tight communication integration between badge and Add-on to create SAOV3, a new SAO standard that puts connectivity right at the forefront. ANSM, our framework to create silky smooth pixel animations and interfaces for embedded systems, is ready for everyone to use. We are even releasing our circuit and driver to make the SSD1106 OLED update smoothly and enables 4-level greyscale on it.

Speakers: Adam Batori, Kevin Colley, Robert Pafford, Lillian Ash Baker

SpeakerBio: Adam Batori

No BIO available

SpeakerBio: Kevin Colley

No BIO available

SpeakerBio: Robert Pafford

No BIO available

SpeakerBio: Lillian Ash Baker

No BIO available

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Beholden to No One: The Nix Override Ladder

Tags: Nix Vegas Community | Creator Talk/Panel

When: Saturday, Aug 8, 10:45 - 10:59 PDT

Where: LVCCW Level 1 Hall 4 1310 (Nix Vegas Community) - [Map](#)

Description:

Home Assistant ships a warning that your install "will not work after 2026.11." DuckStation detects NixOS four different ways and fatally errors your build on purpose. A maintainer won't merge the one-line word-wrap fix you've needed for a year. On most platforms your options are comply or quit. On Nix, everything between you and the source is negotiable.

This talk is a guided tour up the override ladder, from module options and `mkForce` to `overrideAttrs`, `fetchpatch`-ing unmerged PRs, overlays, and finally patching `nixpkgs` itself. The stories along the way are real and primary-sourced: sabotaged npm packages, the `xz` backdoor, the `youtube-dl` DMCA takedown, rug-pull relicensing, and the `nixpkgs` patch literally named `nixos-was-never-supported.patch`.

SpeakerBio: Daniel Baker

Daniel Baker is a developer, engineer, and mathematician passionate about reproducible software. An active NixOS community member and educator, he authored the NixCon NA 2024 Nix module system workshop and `nixos-modules-lessons`. He serves on the NixOS Marketing Team and helps organize both Nix Vegas and Planet Nix. He believes any system worth building is worth rebuilding, bit for bit.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Blacks In Cyber Village - Saturday - 10:00-10:55 PDT

Title: Being Black While Hacking: The Unofficial Survival Guide

Tags: Blacks In Cyber Village | Creator Talk/Panel

When: Saturday, Aug 8, 10:00 - 10:55 PDT

Where: LVCCW Level 3 W322-W324 (BIC Village) - [Map](#)

Description:

In an industry that frequently highlights a massive skills gap, Black professionals are dramatically underrepresented in cybersecurity. This talk uses sharp humor and real-world experiences to explore the realities of being Black in the hacking community. It addresses challenges like the "only one in the room" tax, costly certifications, unconscious bias in hiring, and the emotional labor of code-switching. Attendees will gain insights into systemic barriers and learn how resilience and community, inspired by trailblazers like Camille Stewart Gloster and Tennisha Martin, can overcome rigged systems. This session also challenges allies and leaders to sponsor talent, improve hiring processes, and understand why increasing Black representation is essential for equity and innovation in cybersecurity.

SpeakerBio: Dr. Louis DeWeaver III, Cybersecurity Consultant at Marsh McLennan Agency (MMA)

Dr. Louis DeWeaver is a battle-tested Cybersecurity Consultant at Marsh McLennan Agency (MMA) with over 20 years of real-world experience in the trenches. They hold a hard-earned academic arsenal: an Associate of Applied Science in Information Technology, a B.S. in Information Systems Security (2011), an M.S. in Information Assurance (2016), and a Doctor of Computer Science specializing in Cybersecurity (2021). Dr. DeWeaver doesn't just collect credentials they weaponize them. They serve on the MITRE Engenuity ATT&CK® Evaluations Community Advisory Board, helping define how organizations should actually defend against real adversaries. A proven competitor, they crushed the ONCD Badge Challenge at DEFCON 31 and 32, and in 2025 took down the Policy Village CTF badge created by former ONCD staff. Blunt, high-energy, and unapologetically direct, Dr. DeWeaver has delivered hard-hitting talks at Black Hat, DEF CON, GrrCon, and other major security events. They don't sugarcoat the industry's failures they call them out and show you how to survive (and win) anyway.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Below the Threshold: Real-World APT Tradecraft for Full-Spectrum Compromise

Tags: Red Team Village | Misc

When: Saturday, Aug 8, 17:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 309 (Red Team Village) Workshop Stage 2 - [Map](#)

Description:

This talk aims to demonstrate the modus operandi of an APT focused on full organizational compromise, revealing how such operations actually function in practice — not through isolated tools or techniques, but through the decision-making model that guides every action over time.

Rather than focusing on direct exploitation or individual methods, this session shows how advanced operators structure their actions around continuity, predictability, and behavioral alignment with the target environment. Attacks are not treated as disruptive events, but as controlled sequences of decisions designed to remain coherent and below the threshold of attention.

The presentation walks through a real RedOps engagement from a strategic perspective, highlighting how each step is evaluated in terms of detection probability, behavioral deviation, and operational impact, ensuring the operation remains stable and does not generate relevance over time.

Instead of teaching specific techniques, the talk focuses on analyzing how and why certain strategies are chosen, revealing the underlying principles that drive advanced operations in complex environments.

The narrative is built around three distinct operational tracks conducted within the same organization, which, when combined, enabled full compromise:

- CloudOps — decisions and paths that led to the compromise of cloud resources, including external dependencies and supply chain vectors;
- HybridOps — integration of physical, human, and logical layers, including physical intrusion and contextual exploitation of the corporate environment;
- FinancialOps — understanding of financial and operational processes that enabled the execution of validated fraud without generating meaningful alerts;

Across these three domains, the session demonstrates how cloud, physical, and financial layers can be exploited in a coordinated manner while maintaining consistency with expected system behavior.

As a central part of the session, a real operation conducted by our company will be presented, in which an organization was fully compromised through a coordinated, multi-layered approach. The scenario includes:

- exploitation of a 0day in a physical intrusion context, enabling continuous presence within the environment for 30 days without detection, including a 0-click account takeover scenario;
- progression from an initial phishing vector to full compromise of cloud assets, including resource abuse within well-mapped compromised accounts;
- analysis of critical business services and processes, resulting in confirmed financial fraud through the exploitation of a client-side trust model in a payment system, with direct reputational impact;

In this case, there was no single event that defined the attack, but rather a sequence of controlled and coherent actions that blended into normal operations, enabling full control without triggering traditional detection mechanisms.

The goal of this talk is to provide security professionals with a practical and structured understanding of how APTs actually operate, offering deeper insight into how decisions are made throughout a real-world operation.

The key takeaway is that APT operations are not effective because they are invisible, but because they do not behave like something that deserves attention.

Speakers: Jonathan Coradi, Oliveira Junior

SpeakerBio: Jonathan Coradi

Jonathan Coradi is a RedOps Tech Lead at Hakai Offensive Security, with over 7 years of experience in offensive security. He has led offensive operations across industrial, financial, and banking sectors in Brazil, specializing in advanced penetration testing, Red Team simulations, and physical intrusion engagements. Jonathan is also an elite Bug Bounty Hunter — currently ranked Top 1 on BugHunt — and has reported critical vulnerabilities to companies like Microsoft, Uber, and Mercado Livre, among others.

SpeakerBio: Oliveira Junior

Oliveira Lima is the founder of Hakai and has over 15 years dedicated to the field of cybersecurity, focusing on penetration testing and Red team operations. As a researcher, he has reported numerous vulnerabilities in large companies such as Trend Micro, CISCO, Dlink, etc. Additionally, he has registered more than 40 CVEs. Oliveira continues to be part of the team leading Red team operations.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Bug Bounty Village - Saturday - 12:30-13:30 PDT

Title: Better Bug Hunting on AI Products: A VRP Lead's Perspective

Tags: Bug Bounty Village | Creator Talk/Panel

When: Saturday, Aug 8, 12:30 - 13:30 PDT

Where: LVCCW Level 2 W206-207 (Bug Bounty Village) - [Map](#)

Description:

At Google, we receive hundreds of reports per week (not exaggerating) that claim to identify vulnerabilities in our AI products. However, only a tiny fraction of those (<1%!) will receive a reward. But there is hope! When we break down the reasons so many reports are rejected, nearly all of them fall into a few common categories that make them invalid. Join the Technical Lead of Google's AI Vulnerability Reward Program to walk through these common pitfalls, learn how to bug hunt more effectively on AI products, and hopefully, take home more bounties for your efforts. Outline I. Introduction Self intro, discuss the interest in AI VRP, introduce the problem of low success rates for researchers II. Overview of Google AI VRP - Brief program history, overview of triage/reward process - Explain VRP scope/rewards: In-Scope: Security vulnerabilities (Rogue Actions / Sensitive Data Exfiltration); Some AI Abuse categories Out-of-Scope: "AI slop," simple alignment bypasses, or jailbreaks that do not result in a direct security impact on user data. III. Common Mistakes - Jailbreaks/Safety: Getting an LLM to generate "bad" content is not a security vulnerability we reward through the program (please report in-product!). - Self-pwns: Reports are over-reliant on social engineering or have unconvincing attack scenarios - Ignoring Context: Misunderstanding "sensitive data" versus expected model behavior. IV. Better Bug Hunting - Direct and Indirect Prompt Injection: Reviewing (un)successful AI VRP reports - Our programs look for indirect prompt injection attacks; this isn't always easy to understand - Note: This section will include details from a recently rewarded and disclosed AI VRP report [details TBC pending researcher/corporate comms approval] - Clear and Actionable Reporting: - We want to help teams fix bugs quickly; you can help us do that by writing clear and actionable reports - Reproduction can be challenging due to non-determinism V. Conclusion / Q&A

SpeakerBio: John Kotheimer, Senior Security Engineer, Google

John is a Senior Information Security Engineer and Technical Lead of the AI Vulnerability Reward Program (AI VRP) at Google in New York City. John has significant experience operating bug bounty programs—including a previous role as TL of the Abuse Vulnerability Reward Program at Google—as well as a background in infrastructure security, red teaming, and incident response. As AI VRP lead, John oversees the triage of hundreds of AI bug reports submitted to the program every week. John also coordinates the panel that determines rewards for accepted AI bugs at Google and helps plan and run many of Google's bugSWAT live hacking events. Before joining Google in 2019, John was an information security consultant at Mandiant and completed graduate study at Carnegie Mellon University. Outside of work, he enjoys travel, craft beer, and riichi mahjong.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: BewAIre: Detecting Malicious Pull Requests at Scale with LLMs

Tags: Middle Easterns & Africans in Cyber Security (MEACS) | Creator Talk/Panel

When: Saturday, Aug 8, 13:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 4 1306 (Middle Easterns & Africans in Cyber Security (MEACS) Community) - [Map](#)

Description:

As AI coding assistants accelerate software development, the volume of pull requests at Datadog has grown to nearly 10,000 per week, increasing the risk that malicious changes slip through due to review fatigue. To address this, Datadog built BewAIre, an LLM-powered code review system designed to identify malicious source code changes introduced by threat actors. By reducing approval fatigue for developers while increasing friction for attackers, BewAIre guides human reviewers to the areas where judgment matters most, without slowing developer velocity.

In this breakout session, Andrew Krug, Head of Security Advocacy and Research will share why BewAIre was built, how it evolved from a hackathon experiment into a production-grade internal system, and the key architectural decisions and trade-offs involved along the way. They will discuss what worked, what didn't, and the limitations the team encountered when applying LLMs to security-critical workflows.

They will also cover how BewAIre is now being integrated into Datadog Code Security, and what it takes to turn an internal engineering tool into a product capability used at scale. Attendees will leave with practical lessons on building, hardening, and productizing LLM-powered systems and how you can use LLMs to minimize the security risks introduced by the new LLM-code-generation paradigm.

SpeakerBio: Andrew Krug

No BIO available

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Noob Community - Friday - 14:00-15:20 PDT

Title: Beyond Heatmaps: Hands-On Cyber Risk Quantification with FAIR

Tags: Noob Community | Creator Workshop

When: Friday, Aug 7, 14:00 - 15:20 PDT

Where: LVCCW Level 1 Hall 4 1417 (Noob Community) - [Map](#)

Description:

Cybersecurity has its own language, and business has its own language, and most of the time we're not speaking either of them well. The people who learn to translate between the two are the ones who get listened to, get funded, and get promoted. That's the craft Tony is teaching you in this session.

SpeakerBio: Tony Martin-Vegue

No BIO available

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Bug Bounty Village - Friday - 17:00-17:59 PDT

Title: Beyond Normalization: The Expanding Unicode Attack Surface

Tags: Bug Bounty Village | Creator Talk/Panel

When: Friday, Aug 7, 17:00 - 17:59 PDT

Where: LVCCW Level 2 W206-207 (Bug Bounty Village) - [Map](#)

Description:

Unicode exploitation does not end with normalization. Modern web applications process input through layered pipelines: URL decoding, UTF-8 validation, WAF transformations, framework parsing, surrogate handling, database collation, HTML entity decoding, and increasingly, LLM preprocessing. Each layer implements subtly different assumptions about character validity and equivalence. When those assumptions diverge, security boundaries fail. Building off our popular Black Hat USA 2025 Unicode Briefing, we have continued our research into the complex world of Unicode processing. This research exposes a new class of Unicode pipeline vulnerabilities that extend far beyond canonical normalization issues. We demonstrate how attackers can weaponize illegal UTF-8 sequences to break RE2 validation, exploit surrogate-to-replacement conversions (U+FFFD) to alter semantics, abuse hex overflows to generate filtered characters, and bypass **Host/Secure** cookie protections via Unicode whitespace desynchronization. We show how MySQL zero-weight collation rules enable filter bypasses even after normalization, how WAF/browser canonicalization mismatches lead to XSS and RCE (including analysis of CVE-2025-55182), and how invisible Unicode variation selectors can jailbreak LLMs or conceal supply chain malware. Using real-world telemetry, live demonstrations, tooling updates and hands-on lab environments, this Briefing reframes Unicode as a distributed parsing vulnerability class, not a character encoding footnote. Unicode is no longer just a normalization problem. It is an architectural attack surface.

Speakers:Ryan "ryancbarnett" Barnett,Isabella "4ng3lhacker" Barnett

SpeakerBio: Ryan "ryancbarnett" Barnett, Senior Threat Research Manager, Akamai

Ryan Barnett is a Senior Threat Research Manager leading the Akamai App and API Protector (WAF) product. He also acts as a triager on Akamai's and customers' bug bounty programs. In addition to his primary work at Akamai, he is also a former Faculty Member for the SANS Institute, a WASC Board Member and OWASP Project Leader for: ModSecurity Core Rule Set (CRS) Web Hacking Incident Database (WHID). Mr. Barnett has also authored two web security books: Preventing Web Attacks with Apache (Pearson) and The Web Application Defender's Cookbook: Battling Hackers and Defending Users (Wiley).

SpeakerBio: Isabella "4ng3lhacker" Barnett

Isabella Barnett is a Software Engineering Intern at Akamai and a junior at George Mason Honor's College studying Cyber Security Engineering.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Beyond NPPSPY: Harvesting Credentials via Windows Credential Provider Framework

Tags: Red Team Village | Misc

When: Sunday, Aug 9, 10:00 - 10:59 PDT

Where: LVCCW Level 1 Hall 1 309 (Red Team Village) Workshop Stage 1 - [Map](#)

Description:

For years, Red Teams have relied on techniques like NPPSpy and LSASS dumping for credential harvesting. But as EDRs and defenders get smarter, these traditional paths are heavily monitored and immediately flagged. What if we could intercept credentials right at the source—the Windows Logon UI—while seamlessly bypassing Application Control solutions?

In this talk, we will journey deep into the arcane world of the Windows Credential Provider Framework and COM (Component Object Model) architecture. I will demonstrate how to build a stealthy "Middle-Man" Credential Provider that wraps around the default Windows Password Provider. By abusing interfaces like `ICredentialProviderFilter` and intercepting methods like `GetSerialization`, we can silently harvest both cleartext passwords and serialized authentication payloads.

We'll explore the COM "chicken-and-egg" instantiation process, the operational security considerations of operating inside `logonui.exe`, and most importantly, how this technique achieves a complete bypass of AppLocker by proxying execution through a trusted system process. Finally, we'll discuss its limitations against strict WDAC policies and how defenders can hunt for this elusive persistence mechanism.

Research Motivation & Core Concept

The core insight of this research is moving away from the highly monitored Network Provider registry keys (`HKLM\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\NetworkProvider`) and LSASS memory space. Instead, this research leverages the Windows Credential Provider Framework. By writing a custom COM DLL, we can create a "wrapper" around the native Windows Password Credential Provider (`{60b78e88-ea88-445c-9cfd-0b87f74ea6cd}`).

To avoid drawing suspicion, the user must not see two password fields. This research utilizes the `ICredentialProviderFilter` interface to explicitly filter out (hide) the default Windows provider, leaving only our malicious wrapper.

Technical Insights & Evasion Mechanics

- COM Interface Abuse:** The talk details the exact implementation of `IUnknown`, `IClassFactory`, `ICredentialProvider`, and `ICredentialProviderCredential` required to successfully trick `logonui.exe` into loading the malicious provider.
- Data Harvesting:** I will break down how to extract cleartext passwords by intercepting the `SetStringValue` method, and how to capture serialized payloads (like NTLM hashes/Kerberos material) by intercepting `GetSerialization` before passing execution back to the native provider.
- AppLocker vs. WDAC:** A major finding of this research is Application Control bypass. Because the custom DLL is loaded by `logonui.exe` (a highly trusted, system-level process), AppLocker is completely bypassed. However, I will also transparently discuss WDAC: under strict Enforce Mode, WDAC's CodeIntegrity checks will successfully block the unsigned DLL (Event 3033), making this a great comparative study of AppLocker vs. WDAC for defenders.
- OpSec Constraints:** I will cover the developer-side OpSec required, such as compiling with /MT (statically linking the CRT) to avoid `MSVCP140.dll` dependency crashes in the logon screen, and securely saving harvested credentials via XOR encryption to `C:\Windows\Temp`.

Target Audience

- Red Teamers looking for stealthy persistence and credential harvesting techniques;
- Blue Teamers and Security Engineers tasked with tuning EDRs and writing Application Control (AppLocker/WDAC) policies.

SpeakerBio: Sohail Saha

Sohail is a Penetration Tester at Optiv specializing in Windows internals and offsec tool development. Previously a developer at Polygon, they now leverage their software engineering background to build offensive tooling and research OS architecture. When not bypassing security controls or writing C++, he can be found playing guitar, reading, or working on their debut sci-fi novel.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Beyond Spidering: Behavior Driven DAST for Real Application Workflows

Tags: DEF CON Demo Labs | Intermediate | AppSec | DevOps | Offense/Red Team | SecOps | DEF CON Demo Labs

When: Saturday, Aug 8, 12:00 - 12:45 PDT

Where: LVCCW Level 1 Hall 3 901 (Demo Labs Track 5) - [Map](#)

Description:

Modern web apps do not give up their best attack surface to a spider. The interesting routes, state changes, authenticated functions, and business logic usually sit behind real user behavior. This Demo Lab shows how to stop treating DAST like blind crawling and start driving it with realistic browser flows.

The project began as a software quality proof of concept and evolved through collaboration between an engineering team and a red team into a real operational workflow. By routing Selenium based test scenarios through OWASP ZAP, we turn existing web automation into Behaviour Driven DAST: a practical way to capture richer traffic, exercise meaningful application actions, and uncover security findings that isolated scanning often misses.

Current research shows more than 300% increase in observed attack surface and around 25% improvement in vulnerability detection compared with spider-driven analysis alone. The session will walk through the workflow live, show the comparative results, and introduce a new Python library built from this research.

SpeakerBio: Sara "testingSoul" Martinez

Hi, I am Sara! I started my career in 2014 as a Software Validation Engineer for Communication products. During five years I improved my testing skills by working on projects in Telecommunication, Geolocation, Big Data and Power Electronics. In 2019, I started to focus all this quality knowledge on testing Cybersecurity Software products, and then magic just happened. I discovered a whole new world that fascinated me. Since then, I have been working to improve all my Software and Quality skills including Cybersecurity at every step I take.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Beyond Spidering: Behavior Driven DAST for Real Application Workflows

Tags: DEF CON Demo Labs | Intermediate | AppSec | DevOps | Offense/Red Team | SecOps | DEF CON Demo Labs

When: Friday, Aug 7, 13:00 - 13:45 PDT

Where: LVCCW Level 1 Hall 3 901 (Demo Labs Track 5) - [Map](#)

Description:

Modern web apps do not give up their best attack surface to a spider. The interesting routes, state changes, authenticated functions, and business logic usually sit behind real user behavior. This Demo Lab shows how to stop treating DAST like blind crawling and start driving it with realistic browser flows.

The project began as a software quality proof of concept and evolved through collaboration between an engineering team and a red team into a real operational workflow. By routing Selenium based test scenarios through OWASP ZAP, we turn existing web automation into Behaviour Driven DAST: a practical way to capture richer traffic, exercise meaningful application actions, and uncover security findings that isolated scanning often misses.

Current research shows more than 300% increase in observed attack surface and around 25% improvement in vulnerability detection compared with spider-driven analysis alone. The session will walk through the workflow live, show the comparative results, and introduce a new Python library built from this research.

SpeakerBio: Sara "testingSoul" Martinez

Hi, I am Sara! I started my career in 2014 as a Software Validation Engineer for Communication products. During five years I improved my testing skills by working on projects in Telecommunication, Geolocation, Big Data and Power Electronics. In 2019, I started to focus all this quality knowledge on testing Cybersecurity Software products, and then magic just happened. I discovered a whole new world that fascinated me. Since then, I have been working to improve all my Software and Quality skills including Cybersecurity at every step I take.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Beyond the Ceremony: The 2026 Passkey Attack Surface

Tags: DEF CON Official Talk | Demo | Tool

When: Sunday, Aug 9, 11:00 - 11:59 PDT

Where: LVCCW Level 1 Hall 3 1007 (Main Track 2) - [Map](#)

Description:

Passkeys are marketed as phishing-resistant, and the WebAuthn ceremony at their center genuinely is. The catch: almost nobody runs only the ceremony. Roughly five billion passkeys are in active use (FIDO, 2026), yet only about a third of organizations use them as the primary sign-in, so a passkey almost always sits next to a weaker method. The cryptography covers only the ceremony, but the login rides on many moving parts, from the metal to the cloud: authenticator, cross-device transport, client, relying party, cloud sync, and the human who recovers the account. That is where it breaks, more often than the reputation suggests: in a recent audit, all 103 live relying parties tested were vulnerable to at least one server-side attack.

This talk pulls the scattered research into one pass over all of them, one attack per stop that survives a correct ceremony, shown in action, heaviest on the relying party where engagements land, with a suggested testing order and the sources to go deeper. You also get Passkey Editor, a Burp extension that decodes and re-encodes the vendor wrappers that make this traffic unreadable, ships preset ceremony-layer attacks, and lets you craft any relying-party manipulation by hand in intercept and Repeater.

Walk away knowing where passkey deployments break, with a tool to test them.

A curated, non-exhaustive list of the key references behind this talk.

Cultural anchor

- Nishant Kaushik (CTO, FIDO Alliance), Passkeys Are Not Broken. The Conversation About Them Often Is (<https://fidoalliance.org/passkeys-are-not-broken-the-conversation-about-them-often-is/>), September 2, 2025.

Specifications

- W3C Web Authentication Working Group, Web Authentication (WebAuthn) Level 3 (<https://www.w3.org/TR/webauthn-3/>); Level 2 Recommendation (<https://www.w3.org/TR/webauthn-2/>).
- FIDO Alliance, Credential Exchange Format (CXF) and Credential Exchange Protocol (CXP), Working Drafts (<https://fidoalliance.org/specs/cx/cxp-v1.0-wd-20241003.html>), 2024.

Academic

- Louis Jannett, Andreas Mayer, Maximilian Westers, Vladislav Mladenov, Christian Mainka, Jorg Schwenk, The State of Passkeys: Studying the Adoption and Security of Passkeys on the Web (<https://www.usenix.org/conference/usenixsecurity26/presentation/jannett>), USENIX Security 2026.
- Alaa Daffalla et al., A Framework for Abusability Analysis: The Case of Passkeys in Interpersonal Threat Models (<https://www.usenix.org/conference/usenixsecurity25/presentation/daffalla>), USENIX Security 2025.
- Prince Bhardwaj and Nishanth Sastry (University of Surrey), State of Passkey Authentication in the Wild: A Census of the Top 100K Sites (<https://arxiv.org/abs/2602.15135>), PAM 2026 (Springer LNCS 16477).
- Jenny Blessing, Daniel Hugenroth, Ross J. Anderson, Alastair R. Beresford (University of Cambridge), SoK: Web Authentication and Recovery in the Age of End-to-End Encryption (<https://doi.org/10.56553/popets-2025-0113>), PoPETs 2025(3).
- Matteo Scarlata, Giovanni Torrisi, Matilda Backendal, Kenneth G. Paterson (ETH Zurich / USI), Zero Knowledge (About) Encryption: A Comparative Security Analysis of Three Cloud-based Password Managers (<https://zkae.io/>), USENIX Security 2026 (IACR ePrint 2026/058).

- Mazharul Islam, Sunpreet S. Arora, Rahul Chatterjee, Ke Coby Wang, CASPER: Detecting Compromise of Passkey Storage on the Cloud (<https://www.usenix.org/conference/usenixsecurity25/presentation/islam>), USENIX Security 2025.
- Kemal Bicakci, Fatih Mehmet Varli, Muhammet Emir Korkmaz, Yusuf Uzunay, QES-Backed Virtual FIDO2 Authenticators (<https://arxiv.org/abs/2601.06554>), arXiv:2601.06554, January 2026.
- Christian Catalano, Andrea Chezzi, Vita Santa Barletta, Franco Tommasi, Defeating FIDO2/CTAP2/WebAuthn using Browser-in-the-Middle and reflected XSS (<https://link.springer.com/article/10.1007/s11416-025-00556-2>), Journal of Computer Virology and Hacking Techniques 2025.
- Marco Squarcina, Mauro Tempesta, Lorenzo Veronese, Stefano Calzavara, Matteo Maffei, Can I Take Your Subdomain? Exploring Same-Site Attacks in the Modern Web (<https://www.usenix.org/conference/usenixsecurity21/presentation/squarcina>), USENIX Security 2021.
- Marco Casagrande, Daniele Antonioli, CTRAPS: CTAP Client Impersonation and API Confusion on FIDO2 (<https://arxiv.org/abs/2412.02349>), arXiv:2412.02349, 2024.
- Peizhou Chen, Vulnerability Testing for WebAuthn (MSc thesis, University of Twente; companion Burp_FIDO2 extension) (<https://essay.utwente.nl/98532/>), 2024.

Government guidance

- UK National Cyber Security Centre (NCSC), Comparing the security properties of traditional user credentials and FIDO2 credentials for personal use (<https://www.ncsc.gov.uk/paper/traditional-user-and-fido2-credentials-personal-use>), 2026.

Industry data and reports

- FIDO Alliance, The State of Passkeys 2026: Global Consumer and Workforce Report (<https://fidoalliance.org/the-state-of-passkeys-2026-global-consumer-and-workforce-report/>), May 7, 2026.
- FIDO Alliance, World Passkey Day 2025 / Passkey Pledge (over 1 billion people have activated a passkey; 15 billion accounts support passkeys) (<https://fidoalliance.org/fido-alliance-launches-the-passkey-pledge-to-further-accelerate-global-movement-away-from-passkeys>), May 2025.

Industry and practitioner research

- Luke Jennings (Push Security), MFA downgrade: how attackers are getting around phishing-resistant authentication (<https://pushsecurity.com/blog/mfa-downgrade-attacks>), July 2025.
- Carlos Gomez (IOActive), Authentication Downgrade Attacks: Deep Dive into MFA Bypass (<https://www.ioactive.com/authentication-downgrade-attacks-deep-dive-into-mfa-bypass/>), February 2026.
- Netcraft, Phishing After Passkeys: What Attacks to Expect (<https://www.netcraft.com/blog/phishing-after-passkeys-what-attacks-to-expect>), April 2026.
- Maarten Balliauw (Duende Software), Deep Dive: Relying Party ID and origin with Passkeys (<https://duendesoftware.com/blog/20251014-deep-dive-into-relying-party-id-and-origin-with-passkeys>), October 2025.
- Tobia Righi (mastersplinter), Passkey account-takeover research and CVE-2024-9956 (incl. the credential-ID-collision overwrite note) (<https://mastersplinter.work/research/passkey/>), 2025.
- Curtis Brazzell (PhishU), Vaultjacking: One Captured PIN, the Entire Google Password Manager Vault (<https://phishu.net/blogs/blog-vaultjacking-phishing-the-google-password-manager-vault-in-the-phishu-framework.html>), May 2026.
- U-Zyn Chua (uzyn), Passkey has a theft-detection feature, but Apple, Google and Microsoft broke it (<https://uzyn.com/2025/passkey-has-a-theft-detection-feature-but-big-tech-broke-it/>), May 2025.
- Scott Helme, Open-Sourcing passkeys-php: A Security-Focused WebAuthn Library for PHP (<https://scotthelme.co.uk/open-sourcing-passkeys-php-a-security-focused-webauthn-library-for-php/>), May 2026.
- Dennis Kniep, FIDO Cross-Device Phishing (caBLE/hybrid cross-device relay PoC) (<https://denniskniep.github.io/posts/14-fido-cross-device-phishing/>), September 2025.
- William Brown (firstyear), WTF is a passkey (Open Source Security podcast) (<https://opensourcesecurity.io/2026/2026-01-passkey-william-brown/>), January 2026.

Conference talks (forthcoming / concurrent / recent)

- Michael Grafnetter (DSInternals), Pass-the-Passkey family of attacks (<https://www.dsinternals.com/en/black-hat-usa-26-pass-the-passkey/>), Black Hat USA 2026 (forthcoming).
- Nevada Romsdahl and Kam Talebzadeh, SquarePhish 2.0: QR Code + OAuth 2.0 Device Code Flow Phishing for the Primary Refresh Token (<https://disobey.fi/2026/profile/disobey-2026-433-squarephish-2-0-qr-code-oauth-2-0-device-code-flow-phishing-for-primary-refresh-token/>) Disobey 2026.

Relying-party CVEs (public record, some of them)

- CVE-2026-46419, Yubico java-webauthn-server (webauthn-server-core) (<https://www.yubico.com/support/security-advisories/ysa-2026-02/>).
- CVE-2025-26788, StrongKey FIDO Server (<https://nvd.nist.gov/vuln/detail/CVE-2025-26788>).
- CVE-2024-12225, Quarkus quarkus-security-webauthn (<https://nvd.nist.gov/vuln/detail/CVE-2024-12225>).
- CVE-2025-12150, Keycloak keycloak-services, attestation-policy bypass via fmt:none (<https://github.com/advisories/GHSA-7g5x-9c4v-4w5r>).
- CVE-2026-6856, Keycloak, AAGUID-allowlist bypass via packed self-attestation (NVD record not yet published; tracked at the Keycloak issue) (<https://github.com/keycloak/keycloak/issues/48388>).

SpeakerBio: Matteo Giordano, Anvil Secure

Matteo Giordano is an Italy-based offensive security specialist and Security Engineer at Anvil Secure, focused on application penetration testing and offensive research, with a growing focus on AI Red Teaming and GenAI security. For the past year he has researched WebAuthn and passkeys from an attacker's perspective, mapping the real-world attack surface that sits around the protocol's cryptographic core, the work behind this talk.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Beyond the Flag: How CTF Players Become Product Security Engineers

Tags: Red Team Village | Misc

When: Sunday, Aug 9, 10:00 - 10:59 PDT

Where: LVCCW Level 1 Hall 1 309 (Red Team Village) Workshop Tactic Table 5 - [Map](#)

Description:

Abstract:

Capture The Flag competitions are often dismissed as “just games,” but modern Product Security teams increasingly rely on the exact skills they develop: adversarial thinking, vulnerability analysis, exploit chaining, and secure design under pressure. Whether you are an aspiring security professional or an experienced offensive security practitioner, in this session, you will learn a structured CTF-driven learning roadmap for developing practical security skills and will learn how hands-on, real-world customer-facing offensive engagements contribute to building deep product security expertise. We will also cover how AI capabilities are accelerating this journey of learning and securing the systems. Attendees will participate in a hands-on exercise to explore the challenge through the lenses of CTF problem solving, penetration testing, and Product Security.

=====
Introduction: (1 minute)

Session Overview: (2 mins) • During this session, you will see a practical framework to become a trusted partner in building secure applications rather than being a gatekeeper. Starting with a practical framework of learning and approaching CTFs, to using it as an offensive security practitioner to develop stronger application security capabilities. We also see how AI can accelerate and reshape modern security workflows. • In this session, attendees will be given a challenge designed to get hands-on experience of solving the CTF, creating an offensive security report, and sharing recommendations from a product security engineer's perspective to secure the applications/systems. After the session, I will review each participant's approach and award swag to the top performers.

Intended Audience: (2 mins) • Aspiring security professionals • Experienced penetration testers • Security engineers • Students entering cybersecurity

Capture the Flag (7 minutes) • What is CTF? • Why is CTF crucial? • Hands-on experience • Risk-free environment • Collaboration and teamwork • Skills that CTFs actually teach • Avoiding rabbit hole • Structured approach to learn concepts • OWASP Top 10 • Domains: APIs, Web Application, Crypto, Cloud • A few common vulnerability areas to consider: Injection, File Upload Vulnerabilities, AuthN, AuthZ, Remote Code Execution

Penetration Testing (7 minutes) • What is penetration testing? • Map skills learned in CTF to organizational context using different methods (black box, white box, and grey box testing) • What is the focus area: • Effective technical reports that include: • Details on the process: environment considerations, recon, scanning, and exploitation • List of Findings with details about: What exactly is the specific finding, Severity, Impact, How to remediate the finding

• CTF becomes pentesting when you stop asking: • Can I exploit this? • Where can I find the flag? • And start thinking: • What does this mean for customers? • How does it impact their product?

• Note: One starts to build customer trust by helping them with the business context of findings and how to reduce the risk

Product Security Engineer (7 minutes) • Shift in mindset from “find the bug” to “how do we prevent this everywhere? With the knowledge gained from CTF and real-world pentesting.” • Holistic approach of shifting left the security: • Threat Modeling • Implementing Security Best Practices: • Integration of the SAST tool into the CI/CD pipeline • Logging and monitoring • Cloud Configuration reviews • Least privileges • Vulnerability Management Comparison • Compare with the Software Engineer journey to Programming -> Data Structures -> Front End Developer -> Full Stack Developer

Resource: (2 minutes) • Ask the audience for any recommendations that helped them be strong at what they do • Provide resources that I found useful

Recap: (2 minutes) [CTF - “How do I break this to get the flag?” Pentest - “How bad is this?” Product Security Engineer - “How do we prevent this everywhere?”] AI - “How do we move faster without losing depth?”

Task (2 minutes): • Give them details about the challenge environment • Explain to them the expectations • Find the flag • Penetration Test Report • Explain their approach to secure the feature (Secure Design review, SAST recommendation, how would you prevent it across the application?) • The winner will get swag

Key Takeaways: (3 minutes) • Security is not just: • Finding security gaps • Shipping reports • Security engineers become trusted partners when they: • Know the attacker's mindset • Have hands-on experience in ethical hacking • Understand product goals • Understand how systems fail • Gives practical guidance by being part of secure development with developers • Communicate risk clearly • Improve application security at scale

Q&A (5 minutes)

Speakers:Drew Thompson,Monish Alur Gowdru

SpeakerBio: Drew Thompson

Drew Thompson is a Principal Consultant at UltraViolet Cyber, where he specializes in cybersecurity training, offensive security, and AI-enabled security practices. He designs and delivers hands-on training for security practitioners, develops technical enablement programs, and works closely with consultants and customers to translate emerging attack techniques into practical defensive capabilities. Drew is passionate about making complex security topics accessible through real-world demonstrations, interactive labs, and practical research.

SpeakerBio: Monish Alur Gowdru

Monish Alur Gowdru is a cybersecurity professional with over 6 years of experience in application security and software development. He enjoys helping product teams to secure applications end-to-end throughout the software development lifecycle. He actively contributes to the cybersecurity community as a speaker, mentor, and judge. His ongoing involvement includes prominent work with DEF CON and BSides Edmonton.

LinkedIn: <https://www.linkedin.com/in/ag-monish/>

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Beyond the Hype: The Real Role of Red Teams in an AI World

Tags: Adversary Village | Creator Talk/Panel

When: Sunday, Aug 9, 11:00 - 11:30 PDT

Where: LVCCW Level 1 Hall 3 1105 (Creator Stage 3) - [Map](#)

Description:

Red Teaming is about thinking and acting like an attacker to improve an organization's defenses. In practice, it is less about flashy exploits and more about providing prioritization signals, validating and improving detection capabilities, and telling compelling stories that drive meaningful security outcomes.

The rise of AI has introduced a new challenge and a new mandate. Organizations are increasingly asking Red Teams to "use AI to hack things" as both attackers and defenders race to understand what AI can and cannot do. To cut through the hype, the role of Red Teams to speak truth to power is more important than ever.

Our responsibility is to separate speculation from reality. To understand the capabilities of AI-powered attackers, assess how well our defenses stand up against them, and evaluate the risks introduced by new AI-driven attack surfaces. By doing so, we help organizations make informed decisions about where to invest, what to defend, and how to prepare for the threats that matter most.

Speakers: Michael Leibowitz, Niranjanaa Ragupathy

SpeakerBio: Michael Leibowitz, Senior Principal Troublemaker, Oracle Red Team

Michael (@r00tkillah) has done hard-time in real-time. An old-school computer engineer by education, he spends his days hacking the mothership for a fortune 100 company. Previously, he developed and tested embedded hardware and software, fooled around with strap-on boot roms, mobile apps, office suites, and written some secure software. On nights and weekends he hacks on electronics, writes CFPs, and contributes to the NSA Playset.

SpeakerBio: Niranjanaa Ragupathy, Security Engineer Manager, Google Red Team

Niru is a Security Engineer and Manager at Google. She leads the Offensive Security team, which focuses on hacking Google to improve its overall security. In her free time, Niru enjoys doodling and creating Capture The Flag (CTF) challenges.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Bug Bounty Village - Friday - 12:30-12:59 PDT

Title: Beyond Theoretical Risk: How Cache Poisoning Escalated to Critical Account Takeover in TikTok's Web Infrastructure

Tags: Bug Bounty Village | Creator Talk/Panel

When: Friday, Aug 7, 12:30 - 12:59 PDT

Where: LVCCW Level 1 Hall 3 1102 (Creator Stage 6) - [Map](#)

Description:

Web cache poisoning is often written off as a class of vulnerabilities with limited real-world impact. Most reported instances only expose non-sensitive user metadata, cause temporary, minor disruptions to static content, or require such narrow, impractical conditions to exploit that they rarely move beyond theoretical proof-of-concept. For TikTok's Vulnerability Management team, this framing shaped our initial approach to triaging cache poisoning submissions for years—until two radical researcher submissions upended that assumption entirely, proving misconfigured web caches can undermine every pillar of the CIA triad (confidentiality, integrity, availability) to enable catastrophic, scalable harm. In this talk, we'll start with a foundational breakdown of web cache poisoning: common misconfigurations (from flawed cache key logic to mishandled origin headers) that enable exploitation, and the limited impact profiles that led our team (and many in the bug bounty ecosystem) to historically deprioritize these flaws. We'll then deep dive into the game-changing submissions that reshaped our security posture and why security teams and bug bounty hunters must re-evaluate how they assess cache poisoning risk—moving past surface-level assumptions about limited impact to audit for hidden, critical exploit pathways. Whether you triage web vulnerabilities, build global web infrastructure, or hunt for bugs at scale, this session will equip you to spot and remediate cache poisoning risks before they're weaponized against your users.

SpeakerBio: Glendon Chong, Tiktok

I am part of the Vulnerability Management team for TikTok. Over the past year, I've been actively involved in web application vulnerability triage, collaborating with security researchers and internal teams to dissect, validate, and remediate a wide spectrum of web-based threats. My work centers on bridging reporter expertise and TikTok's security posture—including in-depth negotiations over CVSS scoring, refining triage workflows for emerging attack vectors, and translating complex vulnerability details into actionable remediations. I bring hands-on experience identifying gaps in modern web architectures, advocating for fair, transparent risk assessment with the bug bounty community, and aligning vulnerability prioritization with our platform's commitment to user safety.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Beyond Your Bookshelf: Hackable eReaders

Tags: IoT Village | Creator Talk/Panel

When: Saturday, Aug 8, 15:15 - 15:59 PDT

Where: LVCCW Level 1 Hall 3 1105 (Creator Stage 3) - [Map](#)

Description:

Kindles, Kobos, Boox and BigMes there's no shortage of eReaders to choose from in 2026, with their paper-like eInk displays designed for one thing: reading books. But under the surface of these minimalist devices is a surprisingly hackable device. From Kindle jailbreaks, to Android apps, to flashing custom firmware. We'll take that dust-gathering device off of your nightstand and onto your lab bench to talk about the vulnerabilities and customisability of these devices.

SpeakerBio: Katie Paxton-Fear, Security Advocate, Semgrep

i used to make applications and now I break them, hacker, bug bounty hunter, and educational YouTuber.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Blacks In Cyber Village - Saturday - 13:00-13:55 PDT

Title: Bias is a Bug: Why Inequality is a Cybersecurity Vulnerability

Tags: Blacks In Cyber Village | Creator Talk/Panel

When: Saturday, Aug 8, 13:00 - 13:55 PDT

Where: LVCCW Level 3 W322-W324 (BIC Village) - [Map](#)

Description:

This thought-provoking session examines how bias in AI systems used across cybersecurity for fraud detection, identity systems, and behavioral analytics can inadvertently create structural weaknesses that adversaries might exploit. We will explore how bias can be introduced through data collection, labeling, and modeling, leading to uneven false positive and false negative rates across different populations. Understanding these inconsistencies is crucial, as they can offer attackers avenues to map detection thresholds and bypass security systems. The session will also connect these security risks to emerging regulatory frameworks like GDPR and the AI Act, demonstrating how compliance needs are aligning with core security practices. Join us to learn why integrating equity into threat modeling, red teaming, and system auditing is essential for robust cybersecurity, moving beyond treating fairness as an afterthought.

SpeakerBio: Dr. Fatou Sankare, Cybersecurity Professional / Community Speaker

Dr. Fatou is a Cyber Engineer and an adjunct professor, dedicated to increasing cyber education, particularly in underestimated communities, through Datacation LLC, which they founded. They are a Certified Ethical Hacker and hold the AWS Machine Learning Specialty Certification.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Social Gatherings/Events - Friday - 21:00-00:59 PDT

Title: BIC R00T ACCESS 2026

Tags: Party | Blacks In Cyber Village

When: Friday, Aug 7, 21:00 - 00:59 PDT

Where: LVCCW Level 3 W322-W324 (BIC Village) - [Map](#)

Description:

Black culture has always shaped the sound of resistance, innovation, and celebration—and at DEF CON, we're bringing that history to the dance floor. Blacks In Cyber invites you to a night where cybersecurity meets the soundtrack of Black history. From the soulful roots of jazz and blues that coded messages of freedom, to the revolutionary pulse of hip-hop and electronic beats that powered digital creativity, every track tells a story.

This party celebrates the pioneers who pushed boundaries—musically, technologically, and culturally. Expect a curated journey through decades of sound: classic grooves, Afro-futurist vibes, and modern cyber-inspired mixes that honor the past while hacking the future. Whether you're a seasoned hacker, a first-time DEF CON attendee, or just here for the vibe, this is your space to connect, celebrate, and move.

Come dance through the timeline. Celebrate culture, community, and code. Blacks In Cyber at DEF CON—where history, rhythm, and innovation collide.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Contests - Friday - 12:00-12:59 PDT

Title: BIC Village Capture the Flag (CTF)

Tags: Blacks In Cyber Village | Blacks In Cybersecurity Village Capture The Flag Competition | Contest

When: Friday, Aug 7, 12:00 - 12:59 PDT

Where: LVCCW Level 3 W322-W324 (BIC Village) - [Map](#)

Description:

The BIC Village Capture the Flag (CTF) is your opportunity to tackle real-world cybersecurity challenges, sharpen your technical skills, and compete alongside students, professionals, and cybersecurity enthusiasts during DEF CON 34. Our CTF is designed to challenge your curiosity, celebrate creative problem-solving, and explore cybersecurity through the past, present, and future.

What to Expect: ' Hands-on cybersecurity challenges ' Challenges for multiple skill levels ' Individual and team-based problem-solving ' Opportunities to learn, compete, and connect with the community

Hack to the rhythm and the beat with Hack Hack Revolution. Have an idea or challenge you want to share with the community? Join Bring Your Own CTF (BYOCTF) and contribute your own challenge to the experience. Bring your laptop, curiosity, and determination. Whether you are chasing the top of the leaderboard or solving your very first flag, there is a place for you at BIC Village. Every flag is a lesson. Every challenge is an opportunity. We will see you at the CTF, featuring challenges created by members of the cybersecurity community and the global diaspora!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Contests - Saturday - 12:00-12:59 PDT

Title: BIC Village Capture the Flag (CTF)

Tags: Blacks In Cyber Village | Blacks In Cybersecurity Village Capture The Flag Competition | Contest

When: Saturday, Aug 8, 12:00 - 12:59 PDT

Where: LVCCW Level 3 W322-W324 (BIC Village) - [Map](#)

Description:

The BIC Village Capture the Flag (CTF) is your opportunity to tackle real-world cybersecurity challenges, sharpen your technical skills, and compete alongside students, professionals, and cybersecurity enthusiasts during DEF CON 34. Our CTF is designed to challenge your curiosity, celebrate creative problem-solving, and explore cybersecurity through the past, present, and future.

What to Expect: ' Hands-on cybersecurity challenges ' Challenges for multiple skill levels ' Individual and team-based problem-solving ' Opportunities to learn, compete, and connect with the community

Hack to the rhythm and the beat with Hack Hack Revolution. Have an idea or challenge you want to share with the community? Join Bring Your Own CTF (BYOCTF) and contribute your own challenge to the experience. Bring your laptop, curiosity, and determination. Whether you are chasing the top of the leaderboard or solving your very first flag, there is a place for you at BIC Village. Every flag is a lesson. Every challenge is an opportunity. We will see you at the CTF, featuring challenges created by members of the cybersecurity community and the global diaspora!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: BigIron.ai: AI-Assisted Exploration and Security Analysis of Mainframe Systems

Tags: AI | DEF CON Demo Labs | Intermediate | Defense/Blue Team | Offense/Red Team | Purple Team | DEF CON Demo Labs

When: Friday, Aug 7, 15:00 - 15:45 PDT

Where: LVCCW Level 1 Hall 3 1003 (Demo Labs Track 3) - [Map](#)

Description:

Most security tools assume Unix or Windows models built around processes, shells, and network services. On mainframe operating systems, authority is determined through control-plane behavior: job submission (JCL/JES), dataset access, library resolution, and transaction context. These relationships are difficult to observe and are systematically misunderstood by modern security teams; creating blind spots that traditional tooling cannot see.

This Demo Lab shows a live MVS 3.8j environment running under Hercules with a browser-based TN3270 interface. Operational artifacts including submitted jobs, spool output, and execution context are captured and mapped into a graph that reveals hidden trust relationships and indirect execution paths.

The demonstration walks a realistic privilege path: TSO user → JCL submission → STEPLIB hijack → APF library execution — showing how inherited authority creates system-level exposure without exploiting a single vulnerability. No shellcode. No memory corruption. Just the system working exactly as designed.

The platform includes 13 automated walkthroughs across 6 control planes (TSO, JES, RACF, CICS, VTAM, PR/SM), an offline LLM for real-time screen interpretation, and a findings engine that maps results to a repeatable assessment framework.

SpeakerBio: Adam "w00t0ck" Toscher

Adam Toscher is a New York–based security engineer and red team operator with over two decades of experience in offensive security, adversary simulation, and automation. Born in New York City and raised upstate, Adam began his career as an “IT vagabond,” starting as a freshman IBM intern porting Linux applications to mainframe systems. That early mainframe work grounded him in large-scale computing, operating systems, and complex enterprise environments before he transitioned into offensive security.

He later held senior security roles at Adobe, Optiv, Accenture, IBM X-Force, and NYC Cyber Command, focusing on realistic adversary emulation, red-team operations, and practical automation.

Most recently, Adam has worked with Cobalt Labs, supporting advanced red-teaming and offensive security engagements for private-sector organizations. Prior to that, he led red-team and adversary simulation work supporting critical public infrastructure with NYC Cyber Command and the FDNY.

His work centers on penetration testing, red teaming, adversary emulation, and security tooling across private-sector and government environments. Outside of security, Adam values balance and lifelong learning, and is an avid reader, runner, swimmer, and gamer.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: BigIron.ai: AI-Assisted Exploration and Security Analysis of Mainframe Systems

Tags: AI | DEF CON Demo Labs | Intermediate | Defense/Blue Team | Offense/Red Team | Purple Team | DEF CON Demo Labs

When: Friday, Aug 7, 16:00 - 16:45 PDT

Where: LVCCW Level 1 Hall 3 1003 (Demo Labs Track 3) - [Map](#)

Description:

Most security tools assume Unix or Windows models built around processes, shells, and network services. On mainframe operating systems, authority is determined through control-plane behavior: job submission (JCL/JES), dataset access, library resolution, and transaction context. These relationships are difficult to observe and are systematically misunderstood by modern security teams; creating blind spots that traditional tooling cannot see.

This Demo Lab shows a live MVS 3.8j environment running under Hercules with a browser-based TN3270 interface. Operational artifacts including submitted jobs, spool output, and execution context are captured and mapped into a graph that reveals hidden trust relationships and indirect execution paths.

The demonstration walks a realistic privilege path: TSO user → JCL submission → STEPLIB hijack → APF library execution — showing how inherited authority creates system-level exposure without exploiting a single vulnerability. No shellcode. No memory corruption. Just the system working exactly as designed.

The platform includes 13 automated walkthroughs across 6 control planes (TSO, JES, RACF, CICS, VTAM, PR/SM), an offline LLM for real-time screen interpretation, and a findings engine that maps results to a repeatable assessment framework.

SpeakerBio: Adam "w00t0ck" Toscher

Adam Toscher is a New York–based security engineer and red team operator with over two decades of experience in offensive security, adversary simulation, and automation. Born in New York City and raised upstate, Adam began his career as an “IT vagabond,” starting as a freshman IBM intern porting Linux applications to mainframe systems. That early mainframe work grounded him in large-scale computing, operating systems, and complex enterprise environments before he transitioned into offensive security.

He later held senior security roles at Adobe, Optiv, Accenture, IBM X-Force, and NYC Cyber Command, focusing on realistic adversary emulation, red-team operations, and practical automation.

Most recently, Adam has worked with Cobalt Labs, supporting advanced red-teaming and offensive security engagements for private-sector organizations. Prior to that, he led red-team and adversary simulation work supporting critical public infrastructure with NYC Cyber Command and the FDNY.

His work centers on penetration testing, red teaming, adversary emulation, and security tooling across private-sector and government environments. Outside of security, Adam values balance and lifelong learning, and is an avid reader, runner, swimmer, and gamer.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Biohacking Village - Friday - 10:00-17:59 PDT

Title: Biohacking Device Lab

Tags: Biohacking Village | Creator Event/Activity

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 408 (Biohacking Village) - [Map](#)

Description:

Get hands-on with real medical devices. Learn to identify vulnerabilities, test security controls, and understand how these critical systems work.

21 devices from 9 different MDMs, including BD, Boston Scientific, Siemens Healthineers, Roche, Solventum, Medtronic, MiniMed, and Philips.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Biohacking Village - Sunday - 10:00-13:59 PDT

Title: Biohacking Device Lab

Tags: Biohacking Village | Creator Event/Activity

When: Sunday, Aug 9, 10:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 1 408 (Biohacking Village) - [Map](#)

Description:

Get hands-on with real medical devices. Learn to identify vulnerabilities, test security controls, and understand how these critical systems work.

21 devices from 9 different MDMs, including BD, Boston Scientific, Siemens Healthineers, Roche, Solventum, Medtronic, MiniMed, and Philips.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Biohacking Village - Saturday - 10:00-17:59 PDT

Title: Biohacking Device Lab

Tags: Biohacking Village | Creator Event/Activity

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 408 (Biohacking Village) - [Map](#)

Description:

Get hands-on with real medical devices. Learn to identify vulnerabilities, test security controls, and understand how these critical systems work.

21 devices from 9 different MDMs, including BD, Boston Scientific, Siemens Healthineers, Roche, Solventum, Medtronic, MiniMed, and Philips.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

The Diana Initiative - Saturday - 11:00-11:10 PDT

Title: Biohacking Village Tour

Tags: The Diana Initiative | Creator Tour

When: Saturday, Aug 8, 11:00 - 11:10 PDT

Where: LVCCW Level 1 South Lobby / Atrium - [Map](#)

Description:

Interested in visiting Biohacking Village but afraid to go by yourself? The Diana Initiative is hosting tours! Follow a volunteer to Biohacking Village and be introduced to the community and activities inside!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Bird Hunting Season: The Final Flight

Tags: DEF CON Official Talk | Demo | Tool | Exploit

When: Saturday, Aug 8, 14:30 - 15:30 PDT

Where: LVCCW Level 1 Hall 3 1007 (Main Track 2) - [Map](#)

Description:

Surveillance tech often operates as a "black box" burdened by systemic technical debt. This session is the capstone of "Bird Hunting Season," an independent, self-funded teardown and research of the Flock Safety ecosystem. What began with an eBay purchase evolved into 51+ vulnerabilities across Raven gunshot detectors, Falcon LPRs, and Picard/Bravo compute boxes.

I detail the project's lifecycle: from hardware root via UART and unauthenticated EDL mode to protocol-layer failures. I demonstrate how broken mTLS, hardcoded Java Keystore secrets, and debugging compilations led to system level escalation. The narrative reaches its climax with an explanation of how I found 63 live production camera feeds exposed without authentication to the public internet.

I also formalize the "Flea Market Supply Chain" attack, detailing how direct communication with upstream SoM manufacturers can bypass months of reverse engineering.

The talk culminates in the release of BirdShot: a 12 module testing framework that incorporates the exploits I've discovered as well as a TensorFlow harness (BirdEye) for hijacking proprietary ML models. I demonstrate how BirdShot automates the journey from a three button physical hotspot trigger to a persistent root shell, proving that when the birds are watching you, you can watch them back.

[1] Gaines, J. (2026). Examining the Security Posture of an Anti-Crime Ecosystem. Zenodo. DOI: 10.5281/zenodo.17584876

[2] Gaines, J. (2025-2026). Bird Hunting Season: Anti-Crime Ecosystem Research Repository. GitHub.
<https://github.com/GainSec/anti-crime-ecosystem-research>

[3] MITRE/CWE. ES2510-692960d9: Improper Entitlement/Authorization for Protected Artifact Access. (Submission Pending/Accepted).

[4] <https://github.com/justcallmekoko/ESP32Marauder/wiki/Flock-Sniff>

[5] <https://github.com/justcallmekoko/ESP32Marauder/wiki/flock-wardrive>

[6] <https://github.com/colonelpanichacks/flock-you>

SpeakerBio: Jon "GainSec" Gaines

Jon "GainSec" Gaines is an offensive security researcher, leader and "lifelong hacker" with over a decade of experience hacking all types of technologies for international organizations. By day, he serves as a Senior Security Engineer at Anduril, where he hacks next generation defense systems, following a career of Principal and Managing roles at security firms like NetSPI.

Jon has independently disclosed over 50 CVEs spanning critical infrastructure, hardware, web applications, software, mobile applications, and embedded systems. His technical research has been featured in Phrack Magazine and he maintains a diverse output of open-source projects, ranging from automated PCB hardware hacking tools to control in depth offensive agent governance frameworks. Beyond the lab, he also serves as an adjunct instructor at Herkimer College, where he is dedicated to mentoring the next generation of offensive researchers.

Jon remains committed to lifting the community through technical transparency, tooling, and the meticulous deconstruction of insecure infrastructure.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

DEF CON Training - Tuesday - 08:30-17:30 PDT

Title: Black Belt Pentesting / Bug Hunting Millionaire: Mastering Web Attacks with Full-Stack Exploitation (100% Hands-On)

Tags: DEF CON Training (Paid) (2-day) | DEF CON Training

When: Tuesday, Aug 11, 08:30 - 17:30 PDT

Where: LVCCW Level 2 W224 (Training) - [Map](#)

Description:

SpeakerBio: Dawid Czagan

No BIO available



[Return to Index](#) - Add to Google

- ics [Calendar](#) file

DEF CON Training - Monday - 08:30-17:30 PDT

Title: Black Belt Pentesting / Bug Hunting Millionaire: Mastering Web Attacks with Full-Stack Exploitation (100% Hands-On)

Tags: DEF CON Training (Paid) (2-day) | DEF CON Training

When: Monday, Aug 10, 08:30 - 17:30 PDT

Where: LVCCW Level 2 W224 (Training) - [Map](#)

Description:

SpeakerBio: Dawid Czagan

No BIO available



[Return to Index](#) - Add to Google

- ics [Calendar](#) file

The Diana Initiative - Saturday - 12:50-12:59 PDT

Title: Blacks In Cyber Village Tour

Tags: The Diana Initiative | Creator Tour

When: Saturday, Aug 8, 12:50 - 12:59 PDT

Where: LVCCW Level 1 South Lobby / Atrium - [Map](#)

Description:

Interested in visiting Blacks In Cyber Village but afraid to go by yourself? The Diana Initiative is hosting tours! Follow a volunteer to Blacks In Cyber Village and be introduced to the community and activities inside!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Social Gatherings/Events - Friday - 19:00-00:59 PDT

Title: BlanketFort Con

Tags: Party

When: Friday, Aug 7, 19:00 - 00:59 PDT

Where: LVCCW Level 2 W212 (Misc Meeting Room) - [Map](#)

Description:

BlanketFort Con: Come for the chill vibes and diversity, stay for the Blanket Fort Building, Cool Lights, Music, and Kid Friendly \ Safe environment. Now with less Gluten and more onesies!

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: BLE Theft Auto: How a Dealer-Installed Anti-Theft System Exposes Over a Million Cars to Theft

Tags: DEF CON Official Talk | Demo | Exploit

When: Sunday, Aug 9, 11:30 - 12:30 PDT

Where: LVCCW Level 1 Hall 3 904 (Main Track 4) - [Map](#)

Description:

Car dealers predominantly in the Southwestern U.S. have been pre-installing "KARR," an aftermarket anti-theft alarm system, in every car they sell. They offer these systems as an upgrade when you purchase your car, giving you smartphone-based control over your car locks and immobilizer; if you decline the offer, the dealer says they will deactivate the system. What they don't tell you: this security system is authenticated by a global shared key, so anyone who recovers that key can remotely control nearby KARR units with a smartphone.

KARR is installed in an estimated 1.4 million cars, and every vulnerable unit shipped with the same authentication key, allowing an attacker with a smartphone to unlock the doors, disable the alarm and immobilizer, and trigger the horn and lights of any KARR-equipped vehicle. The core impact is unauthorized access, which can enable burglary, OBD-II access, and escalation including the key-programmer workflow we will demonstrate; every owner with KARR installed needs to update, including those who declined the upsell or inherited it used.

We'll walk through how we discovered KARR, how KARR ends up in millions of cars, how the attack works end-to-end, and what owners can do to fix it today. We'll also show that the same recipe revealed vulnerabilities in other aftermarket BLE systems.

Our paper: Yibo Wei, Jerry Yu, Sumanth Rao, Mohak Vaswani, Jefferson Chien, Christian Dameff, Nishant Bhaskar, Aaron Schulman, "BLE Theft Auto: Evaluating the Security of Aftermarket BLE-based Automotive Remote Control Systems", USENIX Security 2026. (to appear)

Aftermarket alarms: Ken Munro / Pen Test Partners, "Gone in Six Seconds: Exploiting Car Alarms", 2019.
<https://www.pentestpartners.com/security-blog/gone-in-six-seconds-exploiting-car-alarms/>

Aftermarket alarms: VERSPRITE, "How Hackers Control & Steal Vehicles Remotely" (Carlink remote-start vulnerability).
<https://versprite.com/vs-labs/hacking-remote-start-system/>

Automotive BLE and keyless entry: Xie et al., "Access Your Tesla without Your Awareness: Compromising Keyless Entry System of Model 3", NDSS 2023.
<https://www.ndss-symposium.org/ndss-paper/access-your-tesla-without-your-awareness-compromising-keyless-entry-system-of-m>

Automotive BLE and keyless entry: NCC Group, "Tesla BLE Phone-as-a-Key Passive Entry Vulnerable to Relay Attacks", 2022.
<https://www.nccgroup.com/research/technical-advisory-tesla-ble-phone-as-a-key-passive-entry-vulnerable-to-relay-attacks/>

Automotive BLE and keyless entry: Francillon, Danev, Capkun, "Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars", NDSS 2011.

Foundational automotive security: Koscher et al., "Experimental Security Analysis of a Modern Automobile", IEEE S&P 2010. <https://doi.org/10.1109/SP.2010.34>

Foundational automotive security: Checkoway et al., "Comprehensive Experimental Analyses of Automotive Attack Surfaces", USENIX Security 2011. <https://www.autosec.org/pubs/cars-usenixsec2011.pdf>

BLE application-layer auth: Sivakumaran and Blasco, "A Study of the Feasibility of Co-located App Attacks against BLE and a Large-Scale Analysis of the Current Application-Layer Security Landscape", USENIX Security 2019.
<https://www.usenix.org/conference/usenixsecurity19/presentation/sivakumaran>

Measurement and tooling: WiGLE, Wireless Network Mapping. <https://www.wigle.net/>

Measurement and tooling: ILSpy, open-source .NET assembly browser and decompiler. <https://github.com/icsharpcode/ILSpy>

Speakers: Aaron Schulman, Jerry Yu, Yibo Wei

SpeakerBio: Aaron Schulman, University of California, San Diego

Aaron Schulman is an Associate Professor at University of California, San Diego. His research group works on problems that involve gathering large-scale measurements to test whether assumptions about security, and sometimes reliability, match reality. This work often leads his students to gather data on rooftops, at fast food restaurants, gas stations, and hospitals, and while riding in cars, trains, and airplanes. He earned his PhD in Computer Science from University of Maryland, where he studied Internet reliability, and he did a postdoctoral fellowship at Stanford University, where he investigated bottlenecks in cellular infrastructure. Aaron co-discovered sensitive unencrypted data sent over GEO satellites from cellular providers, governments, militaries, and power grid operators. He also co-developed a Bluetooth credit card skimmer detector that federal and state law enforcement have used to stop millions of dollars in credit card fraud. While in Silicon Valley, he co-founded a company that helped Google improve the battery life of the Chrome web browser. This is his third year attending DEF CON.

SpeakerBio: Jerry Yu

Jerry Yu is a wireless systems software engineer associated with the SysNet research group at University of California, San Diego. He contributed to this work by reverse-engineering the mobile apps behind the aftermarket BLE automotive control systems we studied.

SpeakerBio: Yibo Wei, University of California, San Diego

Yibo Wei is a PhD student at University of California, San Diego, advised by Professor Aaron Schulman. He is the lead author of the forthcoming USENIX Security 2026 paper on BLE Theft Auto (under embargo), an ecosystem-wide study of aftermarket BLE-based automotive remote control systems. He led the reverse-engineering, protocol analysis, population estimation, and disclosure for this work. This will be his first time attending DEF CON.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Blockchain defense, stablecoin attacks, and Web3 OSINT

Tags: Cryptocurrency Village | Creator Talk/Panel

When: Friday, Aug 7, 17:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 3 1103 (Creator Stage 5) - [Map](#)

Description:

In this hour, we bring together international hackers to discuss cutting-edge techniques in cryptocurrency security. Our experts break down how distributed red and blue teams face off against crypto developers to secure stablecoin vaults — and how they translated that daily work into a format suited for the Cryptocurrency Village at DEF CON.

We'll also explore how classic Opensource intelligence (OSINT) techniques are converging with modern financial technology to unmask bad actors and bypass security mechanisms. Finally, the panel reveals the tricks that black hats use to extract unauthorized value from real-world mainnet blockchains, including Bitcoin, Solana, Ethereum, and Monero.

As a bonus, you'll get a first look at our forthcoming DEF CON and Black Hat training course, Breaking and Defending Cryptocurrency. We'll share our design process, plans, and the challenges of building a half-dozen hands-on activities that teach the ins and outs of offensive security as it applies to blockchain-based financial technology.

Speakers: Dinmukhammed "Celestial" Kabiden, Izdihar, KL4R10N

SpeakerBio: Dinmukhammed "Celestial" Kabiden, OSINT Mindset

Dinmukhammed Kabiden, also known as Celestial, is a CTI analyst and Web3 investigator from Kazakhstan focused on OSINT, blockchain investigations, crypto fraud, and cyber threat intelligence. He has experience investigating fake airdrops, wallet-drainer activity, on-chain fund flows, scam infrastructure, and OPSEC mistakes that expose threat actors. He is also the organizer of OSINT Mindset and speaks about practical Web3 investigations, intelligence reporting, and the intersection of off-chain and on-chain evidence.

SpeakerBio: Izdihar, Swarmnetics / cyber673 / Brunei Cyber Security Association

Izdihar is a cybersecurity practitioner who works in penetration testing and tinkers with a homelab in his spare time, where he has been experimenting with running blockchain testnet nodes. His interest in cryptocurrency is mostly about understanding how the infrastructure works. He helps run cyber673, a small grassroots community in Brunei.

SpeakerBio: KL4R10N

Sarthak Taneja is a security professional specializing in detection engineering, threat intelligence, cloud forensics, and incident response across fintech, crypto, and Web3 environments. His work focuses on securing digital asset infrastructure, custody workflows, cloud-native systems, and blockchain-adjacent attack surfaces, with experience investigating advanced threat activity from groups such as Lazarus, Kimsuky, BlueNoroff, and ShinyHunters. He has led initiatives across SOC maturity, Detection-as-Code, zero-trust controls, and purple teaming, and has spoken at international security conferences including DEF CON.

Title: BloodBash: Lightweight CLI Python BloodHound Alternative

Tags: Red Team Village | Misc

When: Saturday, Aug 8, 14:00 - 15:59 PDT

Where: LVCCW Level 1 Hall 1 309 (Red Team Village) Tactic Table 4 - [Map](#)

Description:

BloodHound is great... until your VM dies under Neo4j load, your login expires mid-exam, or you need hybrid AD + Entra ID insights without spinning up servers. Enter BloodBash: a standalone Python tool that ingests SharpHound (v6+) and AzureHound JSON directly, builds a full NetworkX graph in-memory, and spits out attack paths, misconfigs, and abuse suggestions — all offline, in colorful terminal glory. Born from a real OSCP crisis (BloodHound failed hours before exam start — BloodBash saved the DA path), this "vibe-coded" tool now detects shortest paths to high-value targets, ADCS ESC1-8 vulns, RBCD, Kerberoasting, GPO abuses, exposed app secrets/certificates, MFA bypass risks, privileged Entra roles, and unified hybrid attack chains. In this talk, you'll see: The OSCP war story that sparked it Live demo: Drop SharpHound + AzureHound files — instant colorful output, path visualization, abuse commands Key detections walkthrough (on-prem + cloud) Why lightweight CLI > GUI bloat for field ops, labs, and quick checks Roadmap: Metasploit integration, more exports, community features Full open-source on GitHub (<https://github.com/DotNetRussell/BloodBash>) — star it, fork it, break it. Attendees walk away with a new go-to tool for AD/hybrid recon.

SpeakerBio: Anthony Russell, Cyber Security Software Engineer

Anthony Russell, is a senior cyber security engineer with over 13 years of professional experience building software. He has a focus in information security and has been featured in 2600 magazine, on Hak5 and has spoken at both Defcon and DerbyCon multiple times. Favorite things to discuss are blockchain technology, baking custom IoT devices, and everything infosec. You can see more of Anthony's work at SquidHacker.com or Twitter.com/DotNetRussell

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Red Team Village - Friday - 12:00-12:59 PDT

Title: BloodHound OpenGraph Crash Course

Tags: Red Team Village | Misc

When: Friday, Aug 7, 12:00 - 12:59 PDT

Where: LVCCW Level 1 Hall 1 309 (Red Team Village) Workshop Stage 2 - [Map](#)

Description:

In this session, attendees will learn how to design data models and build extensions for BloodHound OpenGraph.

After a presentation where I will go over the core concepts & components of BloodHound OpenGraph and the thought process behind BloodHound data modeling, attendees will design a model and build an extension from scratch based on a provided dataset.

If you like to tinker with BloodHound and are curious about the new OpenGraph features, this session is for you...

Note: Bring your own laptop with BloodHound Community Edition installed

SpeakerBio: JD D

WHOAMI



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Red Team Village - Friday - 13:00-13:59 PDT

Title: BloodHound OpenGraph: Six Degrees of Everything

Tags: Red Team Village | Misc

When: Friday, Aug 7, 13:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 1 309 (Red Team Village) Workshop Tactic Table 6 - [Map](#)

Description:

In this session, we'll give a short demo of the BloodHound OpenGraph platform, and show off some modeling capabilities and how to get started working with it. We will show participants an example using lab data with a fake AD environment and Nessus/Vulnerability data and demonstrate how to integrate other sources of data into the existing graph and how easy it is to get started.

Speakers: Rohan Vazarkar, Wes Miller

SpeakerBio: Rohan Vazarkar

Former pentester and original author of BloodHound, turned developer.

SpeakerBio: Wes Miller

Wes Miller is on the Developer Relations team at SpecterOps, and has worked on many of the core components of BloodHound Community Edition including many of the core features of OpenGraph



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Red Team Village - Friday - 10:00-17:59 PDT

Title: BloodHound Quest

Tags: Red Team Village | Misc

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 309 (Red Team Village) Special/Quest Area - [Map](#)

Description:

BloodHound Based CTF

SpeakerBio: Hugo van den Toorn

Hugo is former Chief Information Security Officer and has now transitioned back to help other organizations understand adversary tradecraft. With over twelve years of experience in the Information Security industry, he has a solid technical and executive background as hands-on security leader.

Hugo has experience with and a keen interest in Social engineering, phishing and physical penetration testing. Nowadays, Hugo takes pride and joy in helping individual team members and the business grow. With a strong technical foundation, Hugo combines his passion for security, teaching and hacking with a drive for continuous improvement and optimization of people, processes and technology.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Contests - Saturday - 10:00-11:59 PDT

Title: Blue Team Village CTF - Project Obsidian

Tags: Blue Team Village | Blue Team Village CTF | Contest

When: Saturday, Aug 8, 10:00 - 11:59 PDT

Where: LVCCW Level 2 W213-217 (Blue Team Village) - [Map](#)

Description:

Join Blue Team Village for a defender-focused Capture the Flag competition centered on forensic analysis, malware activity in containerized environments, and cloud-infrastructure attacks. Participants will investigate container images, reconstruct incidents, and solve challenges ranging from beginner to expert. Challenge tracks include Container & Malware Forensics, Cloud Attack Forensics, and Converged Frontier. Participants can choose safe forensic snapshots or advanced live-malware challenges conducted in an egress-restricted Kubernetes sandbox.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Contests - Friday - 10:00-11:59 PDT

Title: Blue Team Village CTF - Project Obsidian

Tags: Blue Team Village | Blue Team Village CTF | Contest

When: Friday, Aug 7, 10:00 - 11:59 PDT

Where: LVCCW Level 2 W213-217 (Blue Team Village) - [Map](#)

Description:

Join Blue Team Village for a defender-focused Capture the Flag competition centered on forensic analysis, malware activity in containerized environments, and cloud-infrastructure attacks. Participants will investigate container images, reconstruct incidents, and solve challenges ranging from beginner to expert. Challenge tracks include Container & Malware Forensics, Cloud Attack Forensics, and Converged Frontier. Participants can choose safe forensic snapshots or advanced live-malware challenges conducted in an egress-restricted Kubernetes sandbox.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

The Diana Initiative - Saturday - 12:20-12:30 PDT

Title: Blue Team Village Tour

Tags: The Diana Initiative | Creator Tour

When: Saturday, Aug 8, 12:20 - 12:30 PDT

Where: LVCCW Level 1 South Lobby / Atrium - [Map](#)

Description:

Interested in visiting Blue Team Village but afraid to go by yourself? The Diana Initiative is hosting tours! Follow a volunteer to Blue Team Village and be introduced to the community and activities inside!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Blue vs Red Bootcamp: From Attacker Playbooks to Defender Detections

Tags: DEF CON Training (Paid) (4-day) | DEF CON Training

When: Tuesday, Aug 11, 08:30 - 17:30 PDT

Where: LVCCW Level 2 W221 (Training) - [Map](#)

Description:

Speakers: Carlo Anez Mazurco, Mariana Ruiz

SpeakerBio: Carlo Anez Mazurco

Carlo Anez Mazurco is a cybersecurity instructor, consultant, and community leader with more than 15 years of experience across security operations, threat intelligence, incident response, threat hunting, and detection engineering. He is the Founder of IgniteCyber Academy, a DEF CON Training instructor, and an active contributor to Blue Team Village, where he supports Project Obsidian and develops hands-on blue team content for the cybersecurity community.

Carlo specializes in helping defenders translate attacker tradecraft into practical detection and response techniques while responsibly integrating artificial intelligence into modern security operations. His work focuses on creating realistic labs, CTF challenges, and immersive training environments that prepare students for real-world investigations using enterprise telemetry, cloud technologies, and AI-assisted workflows.

He has delivered training and presentations for conferences, universities, government organizations, and commercial teams, with a passion for mentoring the next generation of cybersecurity professionals. His goal is to make complex security concepts approachable through practical demonstrations, collaborative learning, and hands-on exercises that participants can immediately apply in their own environments.

SpeakerBio: Mariana Ruiz

No BIO available

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Blue vs Red Bootcamp: From Attacker Playbooks to Defender Detections

Tags: DEF CON Training (Paid) (4-day) | DEF CON Training

When: Saturday, Aug 8, 08:30 - 17:30 PDT

Where: LVCCW Level 2 W221 (Training) - [Map](#)

Description:

Speakers: Carlo Anez Mazurco, Mariana Ruiz

SpeakerBio: Carlo Anez Mazurco

Carlo Anez Mazurco is a cybersecurity instructor, consultant, and community leader with more than 15 years of experience across security operations, threat intelligence, incident response, threat hunting, and detection engineering. He is the Founder of IgniteCyber Academy, a DEF CON Training instructor, and an active contributor to Blue Team Village, where he supports Project Obsidian and develops hands-on blue team content for the cybersecurity community.

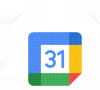
Carlo specializes in helping defenders translate attacker tradecraft into practical detection and response techniques while responsibly integrating artificial intelligence into modern security operations. His work focuses on creating realistic labs, CTF challenges, and immersive training environments that prepare students for real-world investigations using enterprise telemetry, cloud technologies, and AI-assisted workflows.

He has delivered training and presentations for conferences, universities, government organizations, and commercial teams, with a passion for mentoring the next generation of cybersecurity professionals. His goal is to make complex security concepts approachable through practical demonstrations, collaborative learning, and hands-on exercises that participants can immediately apply in their own environments.

SpeakerBio: Mariana Ruiz

No BIO available

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Blue vs Red Bootcamp: From Attacker Playbooks to Defender Detections

Tags: DEF CON Training (Paid) (4-day) | DEF CON Training

When: Sunday, Aug 9, 08:30 - 17:30 PDT

Where: LVCCW Level 2 W221 (Training) - [Map](#)

Description:

Speakers: Carlo Anez Mazurco, Mariana Ruiz

SpeakerBio: Carlo Anez Mazurco

Carlo Anez Mazurco is a cybersecurity instructor, consultant, and community leader with more than 15 years of experience across security operations, threat intelligence, incident response, threat hunting, and detection engineering. He is the Founder of IgniteCyber Academy, a DEF CON Training instructor, and an active contributor to Blue Team Village, where he supports Project Obsidian and develops hands-on blue team content for the cybersecurity community.

Carlo specializes in helping defenders translate attacker tradecraft into practical detection and response techniques while responsibly integrating artificial intelligence into modern security operations. His work focuses on creating realistic labs, CTF challenges, and immersive training environments that prepare students for real-world investigations using enterprise telemetry, cloud technologies, and AI-assisted workflows.

He has delivered training and presentations for conferences, universities, government organizations, and commercial teams, with a passion for mentoring the next generation of cybersecurity professionals. His goal is to make complex security concepts approachable through practical demonstrations, collaborative learning, and hands-on exercises that participants can immediately apply in their own environments.

SpeakerBio: Mariana Ruiz

No BIO available

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Blue vs Red Bootcamp: From Attacker Playbooks to Defender Detections

Tags: DEF CON Training (Paid) (4-day) | DEF CON Training

When: Monday, Aug 10, 08:30 - 17:30 PDT

Where: LVCCW Level 2 W221 (Training) - [Map](#)

Description:

Speakers: Carlo Anez Mazurco, Mariana Ruiz

SpeakerBio: Carlo Anez Mazurco

Carlo Anez Mazurco is a cybersecurity instructor, consultant, and community leader with more than 15 years of experience across security operations, threat intelligence, incident response, threat hunting, and detection engineering. He is the Founder of IgniteCyber Academy, a DEF CON Training instructor, and an active contributor to Blue Team Village, where he supports Project Obsidian and develops hands-on blue team content for the cybersecurity community.

Carlo specializes in helping defenders translate attacker tradecraft into practical detection and response techniques while responsibly integrating artificial intelligence into modern security operations. His work focuses on creating realistic labs, CTF challenges, and immersive training environments that prepare students for real-world investigations using enterprise telemetry, cloud technologies, and AI-assisted workflows.

He has delivered training and presentations for conferences, universities, government organizations, and commercial teams, with a passion for mentoring the next generation of cybersecurity professionals. His goal is to make complex security concepts approachable through practical demonstrations, collaborative learning, and hands-on exercises that participants can immediately apply in their own environments.

SpeakerBio: Mariana Ruiz

No BIO available

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Payment Village - Saturday - 14:00-14:20 PDT

Title: BNPL's Blind Spot: Exploiting Business Logic Flaws in Buy Now Pay Later APIs

Tags: Payment Village | Creator Talk/Panel

When: Saturday, Aug 8, 14:00 - 14:20 PDT

Where: LVCCW Level 2 W204-205 (Payment Village) - [Map](#)

Description:

Buy Now Pay Later has grown from a niche convenience to a \$560 billion global ecosystem used by approximately 380 million people. Klarna, Afterpay, Affirm, and PayPal Pay Later process billions in transactions annually — and every transaction flows through a series of REST API calls. Security research on BNPL has focused entirely on fraud: account takeover, synthetic identity, first-party fraud. No one has looked at the API layer. This talk does.

We systematically test the BNPL payment flow — session creation, authorization, order management, and capture — using public sandbox environments. Our methodology focuses on business logic flaws: scenarios where the API functions exactly as designed but can be abused in ways developers never anticipated.

Confirmed finding: Klarna's capture endpoint accepts any captured_amount value down to 1 cent (\$0.01) on a fully authorized order, with no minimum validation. A \$100 authorized order can be captured for \$0.01 — returning HTTP 201 Created with Klarna-Order-Validation: Valid. In vulnerable merchant implementations, customers receive goods while only \$0.01 is collected — a \$99.99 financial loss per transaction.

Attendees will leave with a practical attack methodology for BNPL integrations, an open-source reference implementation (vulnerable + patched), and a merchant-side security checklist.

SpeakerBio: Furkan Fatih Demir, Independent Security Researcher & Penetration Tester, Barikat Cybersecurity

Conducts authorized security assessments across financial services, aviation, public sector and education, focused on business-logic vulnerabilities that evade conventional tooling.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Game Hacking Village - Friday - 16:00-16:59 PDT

Title: Bobba! A Complete History of Habbo Hotel Private Servers from Shockwave to HTML5

Tags: Game Hacking Village | Creator Talk/Panel

When: Friday, Aug 7, 16:00 - 16:59 PDT

Where: LVCCW Level 1 Hall 1 211 (Game Hacking Village) - [Map](#)

Description:

SpeakerBio: InsiderPHD

No BIO available



[Return to Index](#) - Add to Google

- ics [Calendar](#) file

Car Hacking Village - Saturday - 10:00-16:59 PDT

Title: Bomb Bot Challenge

Tags: Car Hacking Village | Creator Event/Activity

When: Saturday, Aug 8, 10:00 - 16:59 PDT

Where: LVCCW Level 1 Hall 2 701 (Car Hacking Village) - [Map](#)

Description:

In conjunction with the talk, "Hacking the Bomb Bot: How I Learned to Stop Worrying and Love the Boomba", attendees have the opportunity to operate a bomb disposal robot. For those up for a challenge, you'll have a limited amount of time to interact with the robot and test your handling skills. The attendees with the best times will be invited back Sunday morning for a face-off challenge.

The winner will get their very own PackBot 510 to take home!

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Car Hacking Village - Friday - 10:00-16:59 PDT

Title: Bomb Bot Challenge

Tags: Car Hacking Village | Creator Event/Activity

When: Friday, Aug 7, 10:00 - 16:59 PDT

Where: LVCCW Level 1 Hall 2 701 (Car Hacking Village) - [Map](#)

Description:

In conjunction with the talk, "Hacking the Bomb Bot: How I Learned to Stop Worrying and Love the Boomba", attendees have the opportunity to operate a bomb disposal robot. For those up for a challenge, you'll have a limited amount of time to interact with the robot and test your handling skills. The attendees with the best times will be invited back Sunday morning for a face-off challenge.

The winner will get their very own PackBot 510 to take home!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Book Signing - Aamiruddin Syed

Tags: Vendor Book Signing

When: Saturday, Aug 8, 11:00 - 12:59 PDT

Where: LVCCW Level 1 Hall 4 1300 (Book Signings)-Table 1 - [Map](#)

Description:

SpeakerBio: Aamiruddin Syed

Aamiruddin Syed is a Cybersecurity Professional with over a decade of experience specializing in DevSecOps, Shift-Left Security, Cloud Security, and Internal Penetration Testing. He is the OWASP Agentic AI Supply Chain Project Co-Lead and active contributor to the CSA Agentic AI initiative.

He authored Supply Chain Software Security – AI, IoT, Application Security (Apress/Springer) and has deep expertise in automating security in CI/CD pipelines, infrastructure as code, and cloud hardening. He routinely conducts internal security assessments of critical systems and is known for bridging the gap between security and engineering teams to embed security directly into products.

As recognized advocate for secure development, he is a frequent speaker , delivered workshops and chair sessions at leading industry conferences including RSA Conference, DEFCON, and Black Hat.

--

Author:

1. Fault Detection in Microservice Architectures: Integrating Software Fault Prediction with DevSecOps
2. Supply Chain Software Security: AI, IoT, and Application Security

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Social Gatherings/Events - Friday - 16:00-16:59 PDT

Title: Book Signing - Avinash Majeti

Tags: Vendor Book Signing

When: Friday, Aug 7, 16:00 - 16:59 PDT

Where: LVCCW Level 1 Hall 4 1300 (Book Signings)-Table 2 - [Map](#)

Description:

SpeakerBio: Avinash Majeti

Author:

Cybersecurity: Right Access at the Right Time



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Social Gatherings/Events - Saturday - 16:00-16:59 PDT

Title: Book Signing - Avinash Majeti

Tags: Vendor Book Signing

When: Saturday, Aug 8, 16:00 - 16:59 PDT

Where: LVCCW Level 1 Hall 4 1300 (Book Signings)-Table 2 - [Map](#)

Description:

SpeakerBio: Avinash Majeti

Author:

Cybersecurity: Right Access at the Right Time



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Social Gatherings/Events - Friday - 15:00-16:59 PDT

Title: Book Signing - Avinash Majeti

Tags: Vendor Book Signing

When: Friday, Aug 7, 15:00 - 16:59 PDT

Where: LVCCW Level 1 Hall 4 1300 (Book Signings)-Table 1 - [Map](#)

Description:

SpeakerBio: Avinash Majeti

Author:

Cybersecurity: Right Access at the Right Time



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Social Gatherings/Events - Saturday - 14:00-14:59 PDT

Title: Book Signing - Brandy Smith

Tags: Vendor Book Signing

When: Saturday, Aug 8, 14:00 - 14:59 PDT

Where: LVCCW Level 1 Hall 4 1300 (Book Signings)-Table 2 - [Map](#)

Description:

SpeakerBio: Brandy Smith

Author:

Vegas Hackware, Vol1 self titled and Vegas hackware Vol2 The WonderingRaven's Manifesto



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Social Gatherings/Events - Friday - 13:00-13:59 PDT

Title: Book Signing - Brandy Smith

Tags: Vendor Book Signing

When: Friday, Aug 7, 13:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 4 1300 (Book Signings)-Table 2 - [Map](#)

Description:

SpeakerBio: Brandy Smith

Author:

Vegas Hackware, Vol1 self titled and Vegas hackware Vol2 The WonderingRaven's Manifesto



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Social Gatherings/Events - Saturday - 13:00-13:59 PDT

Title: Book Signing - Christopher DeCarmen

Tags: Vendor Book Signing

When: Saturday, Aug 8, 13:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 4 1300 (Book Signings)-Table 2 - [Map](#)

Description:

SpeakerBio: Christopher DeCarmen

Author:

The Cyber Calendar 2027, Y2K27 Edition



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Social Gatherings/Events - Friday - 11:00-11:59 PDT

Title: Book Signing - Christopher DeCarmen

Tags: Vendor Book Signing

When: Friday, Aug 7, 11:00 - 11:59 PDT

Where: LVCCW Level 1 Hall 4 1300 (Book Signings)-Table 2 - [Map](#)

Description:

SpeakerBio: Christopher DeCarmen

Author:

The Cyber Calendar 2027, Y2K27 Edition



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Book Signing - Cindy Cohn

Tags: Vendor Book Signing

When: Saturday, Aug 8, 13:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 4 1300 (Book Signings)-Table 1 - [Map](#)

Description:

SpeakerBio: Cindy Cohn, Executive Director at Electronic Frontier Foundation

Cindy Cohn is the Executive Director of the Electronic Frontier Foundation. From 2000-2015 she served as EFF's Legal Director as well as its General Counsel. Ms. Cohn first became involved with EFF in 1993, when EFF asked her to serve as the outside lead attorney in *Bernstein v. Dept. of Justice*, the successful First Amendment challenge to the U.S. export restrictions on cryptography. Ms. Cohn is the author of the professional memoir, called *Privacy's Defender* published by MIT Press in March, 2026. She is also the co-host of EFF's award-winning podcast, *How to Fix the Internet*.

--

Cohn first became involved with EFF in 1993, when EFF asked her to serve as the outside lead attorney in *Bernstein v. Dept. of Justice*, the successful First Amendment challenge to the U.S. export restrictions on cryptography. She served as EFF's Legal Director as well as its General Counsel from 2000 through 2015, and she has served as Executive Director since then. She also has co-hosted EFF's award-winning "How to Fix the Internet" podcast, which recently concluded its sixth season. Her professional memoir covering her time at EFF, *Privacy's Defender: My Thirty-Year Fight Against Digital Surveillance*, was published earlier this year by MIT Press.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Book Signing - Cindy Cohn

Tags: Vendor Book Signing

When: Saturday, Aug 8, 11:00 - 11:59 PDT

Where: LVCCW Level 1 Hall 4 1300 (Book Signings)-Table 2 - [Map](#)

Description:

SpeakerBio: Cindy Cohn, Executive Director at Electronic Frontier Foundation

Cindy Cohn is the Executive Director of the Electronic Frontier Foundation. From 2000-2015 she served as EFF's Legal Director as well as its General Counsel. Ms. Cohn first became involved with EFF in 1993, when EFF asked her to serve as the outside lead attorney in *Bernstein v. Dept. of Justice*, the successful First Amendment challenge to the U.S. export restrictions on cryptography. Ms. Cohn is the author of the professional memoir, called *Privacy's Defender* published by MIT Press in March, 2026. She is also the co-host of EFF's award-winning podcast, *How to Fix the Internet*.

--

Cohn first became involved with EFF in 1993, when EFF asked her to serve as the outside lead attorney in *Bernstein v. Dept. of Justice*, the successful First Amendment challenge to the U.S. export restrictions on cryptography. She served as EFF's Legal Director as well as its General Counsel from 2000 through 2015, and she has served as Executive Director since then. She also has co-hosted EFF's award-winning "How to Fix the Internet" podcast, which recently concluded its sixth season. Her professional memoir covering her time at EFF, *Privacy's Defender: My Thirty-Year Fight Against Digital Surveillance*, was published earlier this year by MIT Press.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Social Gatherings/Events - Saturday - 14:00-14:59 PDT

Title: Book Signing - Garrett Gee

Tags: Vendor Book Signing

When: Saturday, Aug 8, 14:00 - 14:59 PDT

Where: LVCCW Level 1 Hall 4 1300 (Book Signings)-Table 1 - [Map](#)

Description:

SpeakerBio: Garrett Gee

Author:

The Hacker Mindset



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Social Gatherings/Events - Friday - 14:00-14:59 PDT

Title: Book Signing - Garrett Gee

Tags: Vendor Book Signing

When: Friday, Aug 7, 14:00 - 14:59 PDT

Where: LVCCW Level 1 Hall 4 1300 (Book Signings)-Table 1 - [Map](#)

Description:

SpeakerBio: Garrett Gee

Author:

The Hacker Mindset



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Social Gatherings/Events - Friday - 14:00-15:59 PDT

Title: Book Signing - Laura Scherling

Tags: Vendor Book Signing

When: Friday, Aug 7, 14:00 - 15:59 PDT

Where: LVCCW Level 1 Hall 4 1300 (Book Signings)-Table 2 - [Map](#)

Description:

SpeakerBio: Laura Scherling

The Future of Hacking: The Rise of Cybercrime and the Fight to Keep Us Safe (July 2025, Hardback Launch; July 2026, Audio Book Launch)



[Return to Index](#) - Add to Google

- ics [Calendar](#) file

Social Gatherings/Events - Saturday - 12:00-12:59 PDT

Title: Book Signing - Laura Scherling

Tags: Vendor Book Signing

When: Saturday, Aug 8, 12:00 - 12:59 PDT

Where: LVCCW Level 1 Hall 4 1300 (Book Signings)-Table 2 - [Map](#)

Description:

SpeakerBio: Laura Scherling

The Future of Hacking: The Rise of Cybercrime and the Fight to Keep Us Safe (July 2025, Hardback Launch; July 2026, Audio Book Launch)



[Return to Index](#) - Add to Google

- ics [Calendar](#) file

Social Gatherings/Events - Saturday - 15:00-15:59 PDT

Title: Book Signing - Mark Foudy

Tags: Vendor Book Signing

When: Saturday, Aug 8, 15:00 - 15:59 PDT

Where: LVCCW Level 1 Hall 4 1300 (Book Signings)-Table 2 - [Map](#)

Description:

SpeakerBio: Mark Foudy

Author:

Neurodiverse Hackers: Unconventional Minds Shape Cybersecurity



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Social Gatherings/Events - Friday - 11:00-11:59 PDT

Title: Book Signing - Nicholas DeMeo

Tags: Vendor Book Signing

When: Friday, Aug 7, 11:00 - 11:59 PDT

Where: LVCCW Level 1 Hall 4 1300 (Book Signings)-Table 1 - [Map](#)

Description:

SpeakerBio: Nicholas DeMeo

Author:

Cyber Defense: The Art of Forging a Sentinel



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Social Gatherings/Events - Friday - 15:00-15:59 PDT

Title: Book Signing - Ted Harrington

Tags: IoT Village | Vendor Book Signing

When: Friday, Aug 7, 15:00 - 15:59 PDT

Where: LVCCW Level 1 Hall 1 215 (IoT Village) - [Map](#)

Description:

Join us Friday, August 7 at 3:00pm for a book signing with co-founder and #1 best selling author Ted Harrington. Each attendee will receive a complimentary signed copy of Hackable, while supplies last. We recommend coming early!

SpeakerBio: Ted Harrington

No BIO available

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Social Gatherings/Events - Saturday - 16:00-16:59 PDT

Title: Book Signing - Thomas Wilhelm

Tags: Vendor Book Signing

When: Saturday, Aug 8, 16:00 - 16:59 PDT

Where: LVCCW Level 1 Hall 4 1300 (Book Signings)-Table 1 - [Map](#)

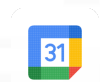
Description:

SpeakerBio: Thomas Wilhelm

Author:

Professional Penetration Testing: Creating and Learning in a Hacking Lab (3rd Edition)

The Basics of Hacking and Penetration Testing (3rd Edition)



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Bootkits Forever: Emulando APTs Modernos desde UEFI hasta el Kernel

Tags: La Villa Community | Creator Talk/Panel

When: Friday, Aug 7, 10:30 - 11:30 PDT

Where: LVCCW Level 1 Hall 4 1416 (La Villa Community) Main Stage - [Map](#)

Description:

Los bootkits UEFI continúan siendo una de las capacidades más avanzadas utilizadas por grupos APT modernos. Su capacidad para ejecutar código antes del sistema operativo, obtener persistencia a largo plazo y operar por debajo de muchas soluciones de seguridad los convierte en una herramienta extremadamente valiosa tanto para atacantes como para equipos de Red Team que buscan emular amenazas reales.

En esta sesión mostraremos cómo utilizar un bootkit UEFI para reproducir cadenas completas de ataque observadas en operaciones reales. Analizaremos el recorrido desde el firmware hasta el kernel de Windows, incluyendo persistencia y despliegue de componentes adicionales de ransomware en el kernel.

La charla incluirá una demostración en directo en la que un sistema Windows moderno será comprometido mediante un bootkit UEFI, mostrando paso a paso cómo este tipo de implantes se instalan y permiten reproducir capacidades observadas en operaciones reales de grupos APT. Además, se compartirán los recursos y proyectos utilizados durante la investigación para que otros equipos de seguridad puedan reproducir los escenarios presentados en sus operaciones diarias.

SpeakerBio: Alejandro Vázquez Vázquez, Independent Security Researcher

Alejandro Vázquez Vázquez es un especialista en técnicas de seguridad ofensiva de bajo nivel, con foco en Red Teaming, Windows Internals y UEFI. A lo largo de su trayectoria ha participado en operaciones de Red Team y emulación de adversarios, además de desarrollar capacidades ofensivas orientadas al estudio y reproducción de técnicas utilizadas por grupos APT modernos. Su trabajo diario se orienta a la creación, análisis y despliegue de implantes capaces de operar por debajo de los mecanismos de seguridad modernos, abarcando desde técnicas pre-boot hasta módulos en kernel y componentes de usuario para persistencia.

Comparte su conocimiento siendo docente en diversos másteres de postgrado de universidades y entidades privadas, donde imparte formaciones en ingeniería inversa, análisis de malware, desarrollo de exploits y desarrollo de herramientas para evasión de soluciones antimalware, acercando la seguridad ofensiva a las nuevas generaciones de profesionales.

Colabora con diversas comunidades centradas en áreas de low-level, como Off By One Security y grupos de DEF CON, conferencia en la que ha sido ponente principal presentando los proyectos Abyss (UEFI Bootkit) y Benthic (Windows Kernel Rootkit). A lo largo de su desarrollo profesional también ha participado en iniciativas de investigación y desarrollo relacionadas con firmware, metahoneypots, análisis de amenazas y plataformas destinadas al estudio de actores maliciosos.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Bug Bounty Village - Saturday - 14:30-15:59 PDT

Title: Bots, Bounties, and Bullshit: An Honest Panel on AI in Hacking

Tags: Bug Bounty Village | Creator Talk/Panel

When: Saturday, Aug 8, 14:30 - 15:59 PDT

Where: LVCCW Level 2 W206-207 (Bug Bounty Village) - [Map](#)

Description:

AI has landed on both sides of the bug bounty table at once. Hackers are being told to use it, programs are drowning in the slop it produces, and a whole new attack surface, agents, RAG pipelines, and tool-calling LLMs, just showed up in scope.

This panel brings together working hackers who run AI in their daily flow, LLM security researchers who break AI for a living, and a moderator who has spent a decade in the scene. In 45 minutes they cut through the hype and get specific: which parts of recon, review, and reporting AI actually handles, how to hack the LLM-backed apps now in scope and get paid for it, and why the real edge isn't ChatGPT but the private agents and skills hackers are quietly building to turn one good idea into a hundred bugs.

Speakers: Ben "NahamSec" Sadeghipour, Vitor "busf4ctor" Falcao Habibe Costa, Joey Melo, Dustin "ph1r3574r73r" Farley, Ads Dawson, Johann "wunderwuzzi23" Rehberger

SpeakerBio: Ben "NahamSec" Sadeghipour

Ben Sadeghipour (NahamSec) is a security researcher, ethical hacker, and educator who has spent more than a decade finding and disclosing critical vulnerabilities in some of the world's largest organizations. As one of the most recognized names in the bug bounty community, he has reported thousands of security flaws and consistently ranked among the top researchers on leading hacking platforms. Beyond his own research, Ben is passionate about lowering the barrier to entry in cybersecurity. Through his widely followed educational content, live streams, and the conferences he founds and organizes, he has helped train a new generation of hackers around the world. His work blends deep technical expertise with a commitment to mentorship and community building. Ben speaks regularly at industry conferences on offensive security, bug bounty hunting, and building a career in cybersecurity.

SpeakerBio: Vitor "busf4ctor" Falcao Habibe Costa, Frontier AI Red Team Operator, BT6

Vitor is an AI security researcher, Community Manager at Critical Thinking, and a Google VRP hunter, named Best AI Researcher at Google bugSWAT. He's part of the BT6 team and hunts bugs full time.

SpeakerBio: Joey Melo

Joey is a Principal Security Researcher at CrowdStrike and a contributor to AI safety programs at OpenAI and Anthropic. He specializes in offensive security research and adversarial analysis of complex systems, with a particular focus on AI/ML infrastructure and large language models. His work has led to the discovery of critical vulnerabilities and novel exploitation techniques, helping organizations better understand and defend against sophisticated threat actors. He has experience across red teaming, exploit development, and designing resilient architectures for high-risk environments. Joey has earned recognition through bug bounty programs and multiple security competitions, with over \$100,000 awarded for vulnerability research. He is also an OSCP, OSCE³ and CRT0-certified professional.

SpeakerBio: Dustin "ph1r3574r73r" Farley, BT6

Dustin Farley has spent more than a decade building software, securing it, and figuring out how to break it. Today, he focuses on AI security, where he spends his time red teaming large language models, AI agents, and other emerging AI systems. His interests include prompt injection, jailbreaks, adversarial testing, and turning weird edge cases into useful security research.

He firmly believes that the fastest way to understand a system is to see how it fails.

SpeakerBio: Ads Dawson, Staff AI Security Researcher, OWASP GenAI Security Project founder

Ads Dawson founded the OWASP GenAI Security Project and led it to flagship status — the fastest in OWASP history. As a Staff AI Security Researcher at Dreadnode, he specializes in exploiting ML and AI systems, harnessing AI for offensive cybersecurity through capability development and exploit development, and conducting red team operations against frontier models for government, military, and tier-1 labs. He is lead author of AIRTBench (arXiv), the first benchmark for autonomous AI red teaming in LLMs, and author of AI Native LLM Security (Packt, 2025).

A senior red team operator with BT6 (the frontier AI red team), ranked #2 in Canada on HackerOne (2025/2026), and selected for Meta's MBBRC live hacking event, Ads is a HackerOne US South Ambassador, BugCrowd Hacker Advisory Board member, MITRE AI Working Group contributor, and leads the OWASP Toronto chapter. He spoke at Bug Bounty Village DC33 on the BT6 AI jailbreaking panel and is also presenting "Exfil Everything: A Year of Stealing Data from AI Agents" at Bug Bounty Village DC34 (schedule pending publication).

SpeakerBio: Johann "wunderwuzzi23" Rehberger

No BIO available

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Noob Community - Sunday - 10:00-10:59 PDT

Title: Break Things, Learn Things: Hands-On Hacking for Beginners (same as Saturday)

Tags: Noob Community | Creator Workshop

When: Sunday, Aug 9, 10:00 - 10:59 PDT

Where: LVCCW Level 1 Hall 4 1417 (Noob Community) - [Map](#)

Description:

Same session as Saturday. You don't need years of experience to start thinking like an attacker—you just need the right environment and someone to show you the ropes. In this hands-on session, Evolve Security Academy completely bypasses the theory to walk you through the fundamentals of ethical hacking in a live, browser-accessible lab environment. You'll adopt an attacker mindset, perform real reconnaissance, run vulnerability scans, and assess live exploits firsthand. Best of all, all registered participants get 7 days of extended access to the CyberLab platform to keep hacking at their own pace after DEF CON.

SpeakerBio: Evolve Security Academy

No BIO available

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Noob Community - Saturday - 10:00-11:20 PDT

Title: Break Things, Learn Things: Hands-On Hacking for Beginners

Tags: Noob Community | Creator Workshop

When: Saturday, Aug 8, 10:00 - 11:20 PDT

Where: LVCCW Level 1 Hall 4 1417 (Noob Community) - [Map](#)

Description:

You don't need years of experience to start thinking like an attacker—you just need the right environment and someone to show you the ropes. In this hands-on, 45-minute session, Evolve Security Academy completely bypasses the theory to walk you through the fundamentals of ethical hacking in a live, browser-accessible lab environment. You'll adopt an attacker mindset, perform real reconnaissance, run vulnerability scans, and assess live exploits firsthand. Best of all, all registered participants get 7 days of extended access to the CyberLab platform to keep hacking at their own pace after DEF CON.

SpeakerBio: Evolve Security Academy

No BIO available

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Red Team Village - Sunday - 12:00-12:59 PDT

Title: Breaking and Defending NEURO: Hands-On AI Stack Attack CTF with Cisco Secure AI

Tags: Red Team Village | Misc

When: Sunday, Aug 9, 12:00 - 12:59 PDT

Where: LVCCW Level 1 Hall 1 309 (Red Team Village) Workshop Stage 2 - [Map](#)

Description:

NEURO is a realistic enterprise AI finance assistant built with an LLM gateway, RAG/vector search, tool calling, MCP integrations, guardrails, audit logs, and a downstream exfiltration simulation.

In this hands-on tactic, attendees will attack and defend the same AI stack from both red-team and blue-team perspectives in our custom CTF.

Participants will work through practical compromise paths including prompt injection, retrieval poisoning, unsafe tool use, MCP trust boundary abuse, and data exfiltration patterns. They will then inspect evidence, review guardrail and audit signals, and apply defensive controls using Cisco Secure AI capabilities such as inspection, scanning, and runtime policy hardening.

The goal is to show how modern AI systems can fail as complete stacks, not just as chat prompts, and how defenders can reason about the full chain from user input to retrieval, tools, model behavior, telemetry, and response controls.

The tactic is designed to fit a 30-120 minute wave with small groups and can be repeated for multiple attendee groups.

SpeakerBio: Jason Ludwig

Jason is a Principle Solutions Architect with over 20 years of experience in software engineering and AI development. He specializes in advanced machine learning systems over many domains, including smart-camera AI for industrial safety, real-time predictive analytics, sentiment analysis, LLMs/Rag, and AI cybersecurity platforms. His work has been featured in Wired, Time, and TED. Jason has successfully led teams at top global organizations like World Wide Technology, Mastercard, and Monsanto, driving the delivery of large-scale, AI-enabled solutions.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Breaking AWS Bedrock: Novel Attack Techniques Against Cloud Infrastructure

Tags: Cloud Village | Creator Event/Activity | Attack

When: Saturday, Aug 8, 13:30 - 14:30 PDT

Where: LVCCW Level 3 W311 (Cloud Village Labs) A - [Map](#)

Description:

Amazon Bedrock is no longer just a research toy. It's embedded in CI/CD pipelines, production applications, and development workflows, often granted sweeping permissions over S3, IAM, and other AWS services. The rapid adoption of agentic AI has reproduced a new class of configuration patterns that security teams haven't caught up with yet. In this hands-on attack lab, Varonis Threat Labs takes you inside real Bedrock deployment patterns observed across AWS environments. Participants will move from initial Bedrock access through data exfiltration, lateral movement, and AWS account compromise, exploiting the same misconfigurations we've found in the wild. No AI hype. No prompt injection gimmicks. This is cloud infrastructure security, and Bedrock just happens to be the way in. Leave with attack paths you can take back to your own environment and the defensive controls to shut them down. **Tal's Bio:** Tal Peleg, also known as TLP, is a senior security researcher and cloud security team lead at Varonis. He is a full-stack hacker with experience in malware analysis, Windows domains, SaaS applications, and cloud infrastructure. His research is currently focused on cloud applications, APIs, and agentic applications.

Speakers: Tal Peleg, Maya Parizer

SpeakerBio: Tal Peleg

Tal Peleg, also known as TLP, is a senior security researcher and cloud security team lead at Varonis. He is a full-stack hacker with experience in malware analysis, Windows domains, SaaS applications, and cloud infrastructure. His research is currently focused on cloud applications, APIs, and agentic applications.

SpeakerBio: Maya Parizer

Maya Parizer is a Security Researcher at Varonis with a passion for cloud security, identity, and data protection, specializing in IaaS and AI. Maya dives deep into every project, thoroughly investigating cloud environments to uncover potential vulnerabilities and stealthy attack techniques. Her experience spans both offensive and defensive disciplines — including CSPM, DSPM, vulnerability research, detection engineering, and product security research in cloud environments.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Breaking BIOS in ATMs

Tags: Payment Village | Creator Talk/Panel

When: Friday, Aug 7, 16:00 - 16:45 PDT

Where: LVCCW Level 2 W204-205 (Payment Village) - [Map](#)

Description:

The analysis begins at Ring -3, advancing toward the positive rings. Starting from the on-screen user perspective imposes too many limitations. The shift in approach was deliberate: rather than assuming a conventional attack vector such as connecting an external device or performing a kiosk-level bypass the decision was made to start from the deepest layers of the system. This compromise is detected for the following reason:

- DMA protection exists at the BIOS level.

The goal of this compromise is to activate PCI/PCIe through BIOS in order to perform a DMA

This section will be referred to as "BIOS Unprotection."

How was this achieved?

Two methods were identified:

A bridge was found that triggers a BIOS configuration reset.

BIOS duplication with encryption validation bypass (enables both Downgrade and Upgrade).

DMA or complete chain will not be shown since it is a delicate topic but BIOS research will be deepened since it does not only apply to ATMs.

SpeakerBio: Arnold Jared Morales Yopez, Senior Team Lead, Grupo Salinas

Self-taught in computer security since age 12; holds a degree in Computer Forensics and Cybersecurity and is pursuing a Master's in AI and Cybersecurity.

--

Desde los 12 años, me he dedicado a la informática con un enfoque especial en la seguridad. Actualmente, a mis 22 años, sigo explorando este mundo con la misma pasión, impulsado por la constante evolución de la tecnología y su interminable curva de aprendizaje.

Cuento con una carrera en Cómputo Forense y Ciberseguridad, actualmente curso una maestría en Inteligencia Artificial y Ciberseguridad.

Certificaciones: CWEE | CAPE |CPTS | EWPTX | CRT0 | eMAPT | OSCP | OSCP+ |CEH V13 | EJPT| HTB prolabs Hades - Cybernetics - Zephyr - APTlabs | MDK



Title: Breaking Ciphers and Zero-Knowledge Proofs

Tags: Cryptocurrency Village | Creator Talk/Panel

When: Saturday, Aug 8, 16:00 - 16:59 PDT

Where: LVCCW Level 1 Hall 3 1103 (Creator Stage 5) - [Map](#)

Description:

Zero-knowledge proofs are a method of demonstrating that a statement is true, without revealing any other information about it, and form the backbone of all the cryptocurrencies we know and love. In this workshop, we will unpack what zero-knowledge proofs really are, how they work, and what they do to ensure that your personal information remains private. A familiarity with basic cryptography is helpful, but not strictly necessary.

Speakers: Luke Szramowski, Freeman Slaughter, Diego "rehrrar" Salazar

SpeakerBio: Luke Szramowski, Stack Wallet

Luke Szramowski is a mathematical researcher, with a Bachelor's Degree in Mathematics and two Master's Degrees, one in Math, with a focus in Number Theory and another in Math with a focus in Coding Theory. In his free time, Luke works on a litany of different math problems, mainly regarding Number Theoretic conjectures and playing all different types of games.

SpeakerBio: Freeman Slaughter, Cypher Stack

Freeman is a cryptographic researcher specializing in zero-knowledge proofs and code-based cryptography. He has co-authored several influential peer-reviewed works, including designing the post-quantum signature scheme CROSS, which is currently under review for government standardization. His work is driven by a strong commitment to advancing the privacy and security of cryptocurrencies such as Monero and Salvium.

SpeakerBio: Diego "rehrrar" Salazar, Cypher Stack

Diego 'rehrrar' Salazar has been around the FOSS and cryptocurrency communities for eight years. He owns and runs Cypher Stack, a company that performs novel research and makes contributions to various FOSS projects. He has organized and managed several villages at defcon, c3, and more.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Breaking Hardware CFI with Sigreturn

Tags: DEF CON Official Talk | Demo

When: Friday, Aug 7, 17:30 - 17:59 PDT

Where: LVCCW Level 1 Hall 3 1007 (Main Track 2) - [Map](#)

Description:

Modern ARM64 systems rely on hardware Control-Flow Integrity (CFI) such as PAC and BTI to kill classic ROP/JOP exploits. Indirect branches must land on valid targets, returns are signed, and arbitrary jumps are supposed to be over.

Except... it isn't.

In this talk, we show that, by design, there is a fundamental gap between POSIX signal handling and hardware CFI. Sigreturn acts as a built-in, kernel-assisted CFI bypass primitive, enabling arbitrary control-flow transfers via crafted signal frames while bypassing CFI enforcement.

We then explore what makes this work in practice on modern Linux and Android systems (including latest Ubuntu and Pixel devices): using sigreturn as a practical exploitation primitive, then pivoting with "cfi-safe stack pivots", abusing missing BTI enforcement on the vDSO, and leveraging GCC's common default settings.

I'll present a PoC showing how these primitives can be chained in classic SROP style, and demonstrate how you can extend COOP/CFOP beyond function-level control to achieve reliable arbitrary code execution, effectively breaking CFI again and again.

References

- SROP
 - ◆ "Framing Signals—A Return to Portable Shellcode", Erik Bosman & Herbert Bos, IEEE S&P 2014. Link: https://www.cs.vu.nl/~herbertb/papers/srop_sp14.pdf
- COOP
 - ◆ "Counterfeit Object-oriented Programming", Schuster et al., IEEE S&P 2015. Link: <https://www.ieee-security.org/TC/SP2015/papers-archived/6949a745.pdf>
- CFOP
 - ◆ "Await() a Second: Evading Control Flow Integrity by Hijacking C++ Coroutines", Marcos Bajo and Christian Rossow, CISPA Helmholtz Center for Information Security, Usenix 2024. Link: <https://www.usenix.org/conference/usenixsecurity25/presentation/bajo>

SpeakerBio: Omri "beta_b0t" Ben Bassat, Tel Aviv University

Omri Ben-Bassat is a vulnerability researcher with over a decade of experience in reverse engineering, vulnerability finding, binary exploitation, and low-level vulnerability analysis, specializing in IoT and embedded systems. He has presented his work at leading security conferences, including Black Hat USA, Black Hat Asia, and RSA Conference, and has delivered awesome hands-on trainings at Black Hat Asia and TyphoonCon. Omri is currently pursuing a master's degree at Tel Aviv University, where his research focuses on applying formal methods to software exploitation.



Physical Security Village - Sunday - 10:00-10:30 PDT

Title: Breaking In, Evil Style: A Guide to Scaring Your CEO

Tags: Physical Security Village | Creator Talk/Panel

When: Sunday, Aug 9, 10:00 - 10:30 PDT

Where: LVCCW Level 1 Hall 3 1104 (Creator Stage 4) - [Map](#)

Description:

You've cloned the keycards, you've bypassed the locks, and you've gotten into the building. Now what?

Convincing people to actually fix the security issues you find is always an uphill battle. It's even worse in the world of physical security, where installing new locks costs more than deploying a software patch. This talk will explore how to make your physical red teaming activity scare the \$hit out of your executives. We'll establish persistence, pivot to the network, steal everything that isn't nailed down, and put dollar amounts to the impacts of your findings.

Along the way, we'll look at some of the techniques used by real-world threat actors that use physical attacks as part of their attack chains, and how you can effectively emulate the most realistic threats to your organization. Your adversaries don't stop after getting in, and neither should you.

SpeakerBio: Andrew Lebedinsky, Security Engineer, Red Team at Microsoft

Andrew Lebedinsky is a security engineer on the Microsoft Red Team. Their fields of interest include covert entry, radio hacking, and digital countersurveillance. In their spare time they can usually be found playing Source Engine-based FPS games and overthinking what to put in "speaker bio" fields.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Breaking into Amazon lockers by any means necessary

Tags: DEF CON Official Talk | Demo

When: Friday, Aug 7, 13:30 - 14:30 PDT

Where: LVCCW Level 1 Hall 3 1007 (Main Track 2) - [Map](#)

Description:

Amazon Lockers are everywhere, handling millions of packages every day. At the same time, thousands of packages get stolen from home porches every year, which made me wonder if the same thing could happen with Amazon Lockers.

This talk is my journey trying to break into them. I started where it made the most sense, BLE. What looked straightforward quickly turned into a series of unexpected turns, with different angles, different ideas, and a lot of time spent chasing paths that didn't go where I thought they would.

This talk walks through that process, the dead ends, the pivots, and the techniques used along the way showing how attacking a system from different angles can expose weaknesses that aren't obvious at first. From protocol reverse engineering and hardware hacking to mobile app security, OSINT, and physical attacks, in the end it's about persistence, understanding how things really work, and not stopping until something gives.

By any means necessary.

All references are pointed in the outline to provide better context.

SpeakerBio: Martin Vigo, Triskel Security

Martín is a cybersecurity expert with 15 years of experience, having helped protect companies such as Apple, Meta, and Salesforce, including work in penetration testing, red teaming, and vulnerability research. He has led teams and worked across mobile and web security, SaaS, cloud environments, and identity and authentication.

He is a frequent speaker at conferences including DEF CON, Black Hat, and CCC, presenting research on phreaking, vulnerabilities in password managers, new OSINT techniques, and reverse engineering of proprietary protocols.

He runs a cybersecurity consulting firm focused on improving organizational cyber resilience via offensive security, research, and public speaking. He is also co-host of the "Tierra de Hackers" podcast.

Martín holds a Bachelor's in Computer Science, a Master's in Software Engineering, and certifications in areas such as hardware hacking, exploit development, infrastructure and mobile security, radio frequency, and OSINT. He contributes to open source projects and collaborates with law enforcement on initiatives to enhance public safety.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Breaking Local AI Runtimes: Exploiting llama.cpp and Ollama

Tags: DEF CON Official Talk | Demo | Exploit

When: Friday, Aug 7, 10:30 - 11:30 PDT

Where: LVCCW Level 1 Hall 3 1007 (Main Track 2) - [Map](#)

Description:

Local LLM runtimes now sit inside phones, desktops, and internal servers, but the layer underneath is still ordinary native code. We analyzed llama.cpp and Ollama across three trust boundaries: JNI, HTTP lifecycle code, and Go/C bindings.

First, in the llama.cpp Android integration, Java can free a native llama_context while native code is still using it. We reclaim the freed 648-byte object, redirect a vtable call, and show code execution in the embedding app. Second, in llama.cpp server, idle model teardown can race active requests, leaving a dangling pointer inside a freed 17,816-byte model allocation. We show remote cross-thread reclaim and attacker-controlled native dereference, then explain the remaining steps to stable RCE. Third, in Ollama, malicious GGUF metadata can push unsafe lengths across the Go/C boundary during quantization, causing C to read past a Go-backed buffer and return heap data to the caller.

This is not a prompt-injection talk. It is about exploiting local AI runtimes as native software: one full exploit, one validated server-side primitive, one disclosure primitive, and the audit patterns that find more.

1. Mergendahl, Louloudis, Vidas. "Cross-Language Attacks." NDSS Symposium 2022.
2. Hussain. "Incubated Machine Learning Exploits." DEF CON 32, 2024.
3. Riancho, Braverman, Demetrio. "Breaking Out of The AI Cage." Black Hat USA 2025.
4. llama.cpp project: <https://github.com/ggml-org/llama.cpp>
5. Ollama project: <https://github.com/ollama/ollama>
6. llama.cpp Android sample: <https://github.com/ggml-org/llama.cpp/tree/master/examples/llama.android>

Speakers: Ofek Itach, Vladimir "G1ND1L4" Tokarev

SpeakerBio: Ofek Itach, Cyera

Security Research Team Lead at Cyera. Focus areas include cloud infrastructure and AI-related platform security. Talks: Black Hat USA 2024, DEF CON 32 (2024), RSA 2024, Sector 2024, INTENT 2024, Black Hat Europe 2024 Arsenal. Earlier work includes AWS internals and cloud attack surface mapping.

SpeakerBio: Vladimir "G1ND1L4" Tokarev, Cyera

Vladimir Tokarev is a vulnerability researcher tech lead at Cyera, specializing in Cloud, IoT/OT, Windows, Linux, and AI vulnerability research and exploit. Talks: Black Hat USA 2024 and 2023, DEF CON 33 Recon Village 2025, CodeBlue 2025, RSA 2024.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Breaking MCP Trust Boundaries: Cross-Server Authority Injection in Agent Toolchains

Tags: Red Team Village | Misc

When: Saturday, Aug 8, 15:00 - 15:59 PDT

Where: LVCCW Level 1 Hall 1 309 (Red Team Village) Workshop Stage 2 - [Map](#)

Description:

Modern MCP deployments assume that low-privilege tools remain low-risk when reviewed independently. In practice, host agents compose outputs across multiple tools and privilege levels, creating authority paths that do not exist in any single server's standalone review.

This workshop demonstrates a compositional offensive primitive in MCP environments: a low-privilege server influencing the parameters of a high-privilege destructive operation through shared planning context.

Attendees will see a controlled lab reproduction where a read-only MCP server shapes the parameters of a privileged SQLite-backed delete operation. The approval prompt shown to the operator accurately describes the final action but omits the upstream provenance that influenced it.

The workshop introduces Urd, an open-source compositional analysis tool for MCP deployments. Urd reconstructs authority flow across servers using runtime tracing and manifest analysis, allowing operators and red teamers to identify undeclared cross-tool influence paths.

The focus of the session is not prompt injection or model jailbreaks. The focus is cross-server authority flow, provenance loss, and workflow-level trust failure in agentic systems.

This session includes a hands-on tactic where attendees reproduce the compositional failure locally, inspect runtime traces, generate divergence findings, and modify the lab to observe how low-trust inputs can influence privileged operations across MCP toolchains.

SpeakerBio: Yevhen Pervushyn

Yevhen “valh4x” Pervushyn is the founder of Red Asgard, a security research firm focused on AI integration security, offensive security, and protocol analysis.

His work focuses on the operational security of agentic systems: orchestration boundaries, authorization flow, provenance, and workflow-level trust failure in AI deployments.

Prior to Red Asgard, he worked in blockchain security auditing and decentralized protocol analysis, experience that directly informs his current research into compositional trust failures in MCP-based systems.

He previously presented MCP security research at the SANS AI Cybersecurity Summit 2026. This session presents new technical research, tooling, and hands-on lab material focused on offensive analysis of MCP orchestration behavior.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Payment Village - Saturday - 12:00-12:59 PDT

Title: Breaking PBKDF - Adversarial Cryptanalysis and Techniques for Hunting Cryptographic Flaws

Tags: Payment Village | Creator Talk/Panel

When: Saturday, Aug 8, 12:00 - 12:59 PDT

Where: LVCCW Level 2 W204-205 (Payment Village) - [Map](#)

Description:

Using decades-old OpenJDK PBKDF flaws, forgotten RFCs, hash collisions, and a few semantic edge cases, we'll compromise multiple cryptographic systems with little more than a handful of carefully chosen values and several “useless” tools.

This talk explores how implementation bugs, legacy compatibility, and architectural assumptions can undermine otherwise sound cryptography—and why the real attack surface is often everything around the algorithm.

SpeakerBio: Ken Pyle, Security Researcher, Bank of America

Cybersecurity researcher, exploit developer and conference speaker focused on vulnerability discovery, reverse engineering and adversarial cryptanalysis; has presented at DEF CON, ShmooCon and RSA Conference.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

DEF CON Training - Monday - 08:30-17:30 PDT

Title: Breaking Physical Access Control: Electrical Fundamentals, RFID Credentials, and Hands-On Offense

Tags: DEF CON Training (Paid) (2-day) | DEF CON Training

When: Monday, Aug 10, 08:30 - 17:30 PDT

Where: LVCCW Level 2 W212 (Misc Meeting Room) - [Map](#)

Description:

SpeakerBio: Red Team Alliance

No BIO available



[Return to Index](#) - Add to Google

- ics [Calendar](#) file

DEF CON Training - Tuesday - 08:30-17:30 PDT

Title: Breaking Physical Access Control: Electrical Fundamentals, RFID Credentials, and Hands-On Offense

Tags: DEF CON Training (Paid) (2-day) | DEF CON Training

When: Tuesday, Aug 11, 08:30 - 17:30 PDT

Where: LVCCW Level 2 W212 (Misc Meeting Room) - [Map](#)

Description:

SpeakerBio: Red Team Alliance

No BIO available



[Return to Index](#) - Add to Google

- ics [Calendar](#) file

Title: Breaking the Chains of Cloud Giants: Building a Fully Autonomous Personal Cloud on NixOS

Tags: Nix Vegas Community | Creator Talk/Panel

When: Saturday, Aug 8, 16:30 - 16:59 PDT

Where: LVCCW Level 1 Hall 4 1310 (Nix Vegas Community) - [Map](#)

Description:

Privacy and digital agency are under siege by dark patterns, aggressive data harvesting, and SaaS monopolies. It's time to reclaim our digital self-determination. This talk demonstrates how to build a production-ready, fully autonomous personal cloud using the declarative power of NixOS. We will explore how to self-host drop-in replacements for mainstream services—including Nextcloud for storage, Vaultwarden for passwords, and Matrix for communication. Attendees will learn how to turn any old PC or cheap VPS into an unbreachable digital fortress featuring automated backups, end-to-end encryption, and complete data isolation. Discover how NixOS makes personal infrastructure reproducible, resilient, and entirely yours.

Speakers: Maksim Kuskov, Mikhail Ilin

SpeakerBio: Maksim Kuskov

Security engineer in Yandex, CTF organizer & player @ HSE IS '29

SpeakerBio: Mikhail Ilin

I am an appsec with a strong background in competitive hacking. Over the years, I have won multiple national Cyber Security Sports Championships and currently serve as an ambassador for the Standoff 365 cybersecurity ecosystem. Beyond traditional technical exploitation, my research focuses on the intersection of clinical psychology and practical social engineering. As a strong advocate for digital self-determination, I view open-source infrastructure and NixOS not just as engineering tools, but as essential defensive shields against platform lock-in and corporate surveillance.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

DEF CON Training - Monday - 08:30-17:30 PDT

Title: Breaking the Cloud Layer - Modern and Practical Attacks on AWS, Azure, GCP, Aliyun, Railway and Vercel

Tags: DEF CON Training (Paid) (2-day) | DEF CON Training

When: Monday, Aug 10, 08:30 - 17:30 PDT

Where: LVCCW Level 2 W208 (Quiet Room with TDI and MHH) - [Map](#)

Description:

Speakers: Anant Shrivastava, Riyaz Walikar

SpeakerBio: Anant Shrivastava

Anant Shrivastava is the founder of Cyfinoid Research and a long time offensive security practitioner with a focus on application, cloud, and supply chain security. He has delivered trainings and talks at Black Hat (USA, Europe, Asia), Nullcon, c0c0n, BSides, Rootconf and multiple other events, and runs projects such as Hacking Archives of India to highlight real work from the security community. His courses are built from real consulting and red team experience, with an emphasis on attack chains that actually show up in the field and defenses that teams can implement the next day.

SpeakerBio: Riyaz Walikar

No BIO available

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

DEF CON Training - Tuesday - 08:30-17:30 PDT

Title: Breaking the Cloud Layer - Modern and Practical Attacks on AWS, Azure, GCP, Aliyun, Railway and Vercel

Tags: DEF CON Training (Paid) (2-day) | DEF CON Training

When: Tuesday, Aug 11, 08:30 - 17:30 PDT

Where: LVCCW Level 2 W208 (Quiet Room with TDI and MHH) - [Map](#)

Description:

Speakers: Anant Shrivastava, Riyaz Walikar

SpeakerBio: Anant Shrivastava

Anant Shrivastava is the founder of Cyfinoid Research and a long time offensive security practitioner with a focus on application, cloud, and supply chain security. He has delivered trainings and talks at Black Hat (USA, Europe, Asia), Nullcon, c0c0n, BSides, Rootconf and multiple other events, and runs projects such as Hacking Archives of India to highlight real work from the security community. His courses are built from real consulting and red team experience, with an emphasis on attack chains that actually show up in the field and defenses that teams can implement the next day.

SpeakerBio: Riyaz Walikar

No BIO available

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Breaking the Ethereum Phone: From BootROM to Wallet Signing Keys

Tags: DEF CON Official Talk | Demo | Exploit

When: Friday, Aug 7, 10:00 - 10:30 PDT

Where: LVCCW Level 1 Hall 3 1007 (Main Track 2) - [Map](#)

Description:

Crypto phones promise the convenience of a mobile OS with hardware-backed key management. We tested that claim on dGEN1, the Ethereum phone marketed for digital-asset custody, and present a full compromise from bootrom to wallet key recovery.

Starting from a bootrom-level misconfiguration, we reverse the modern MediaTek bootchain and introduce a Loader-of-the-Loader technique for patching later boot stages entirely in memory, yielding EL3 code execution without modifying physical flash. From that foothold, we trace how boot-level compromise propagates into the device's lock-screen verification path, enabling offline brute-forcing of the user PIN and recovery of the wallet's primary ERC-4337 signing key. We further show that a separate identity flaw in the asset-claim workflow allows pre-activation theft using identifiers printed on a sealed retail box.

SpeakerBio: Guanxing Wen

Guanxing Wen is a security researcher with over a decade of experience exploiting bootloaders, TEEs, kernels, and IoT systems. He is a top winner of Huawei bug bounty (2021/2022) and is listed in the Ledger Hall of Fame. His research has been presented at Black Hat, MOSEC, INFILTRATE, Summercon, and QPSS. He currently works at CertiK, where he focuses on low-level systems exploitation and blockchain infrastructure.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Breaking the Oracle: Building an Offensive Security Toolkit for OCI

Tags: Demo | Cloud Village | Creator Talk/Panel

When: Sunday, Aug 9, 11:20 - 11:50 PDT

Where: LVCCW Level 3 W313 (Cloud Village Talks) - [Map](#)

Description:

Oracle Cloud Infrastructure (OCI) is arguably one of the lesser-explored major cloud platforms from an offensive security perspective. While OCI shares many familiar IAM concepts with AWS and GCP, its identity architecture—including sentence-based IAM policies, identity domains, dynamic groups, compartment hierarchies, and cross-tenancy permissions—creates authorization relationships and privilege escalation paths that benefit from OCI-specific analysis.

To help tackle these challenges, I built OCInferno, an open-source OCI reconnaissance framework for offensive security assessments. Alongside oci-lexer-parser, an ANTLR-based parser for OCI's sentence-based IAM policies, and OCISigner, a Burp Suite extension for transparently signing OCI API requests, a pentester/blue teamer can automate enumeration, model OCI IAM relationships, and build OpenGraph-based attack paths similar to BloodHound to help visualize privilege escalation opportunities.

This talk will demonstrate how to model OCI IAM relationships and uncover OCI-specific attack paths that are difficult to spot from policy text alone. It will also cover a security issue I uncovered that was acknowledged by Oracle in the June 2026 Critical Security Patch Update under its Security-in-Depth program, illustrating how offensive security research can uncover weaknesses not only in customer environments but in the cloud platform itself. Whether you're new to OCI or already assessing cloud environments, you'll leave with a practical understanding of OCI IAM, identity-domain-aware attack path analysis, and an open-source toolkit for exploring OCI security.

SpeakerBio: Scott Weston

Originally from Southern California and now based in Minneapolis, Scott has six years of experience in information security. As a Labs Researcher at NetSPI, he builds open-source tools and research material focused on cloud security and penetration testing across AWS, GCP, and OCI environments. His tools include gcpwn, ocinferno, oci-lexer-parser, and ocisigner.

In his spare time, he enjoys being a totally fair and impartial D&D Dungeon Master, and holding out hope that San Diego FC will advance to the MLS finals.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Aerospace Village - Friday - 10:00-17:59 PDT

Title: Bricks in the Air

Tags: Aerospace Village | Creator Event/Activity

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 2 700 (Aerospace Village) - [Map](#)

Description:

Step right up to our interactive LEGO aircraft. Can you investigate the aircraft's control system, identify any vulnerabilities, and “hack” beyond its intended functions?

This exercise uses real-world I2C protocols to simulate potential vulnerabilities in an aircraft control system.

No specialized hardware required - all target devices, materials, and interfaces are provided!

No prior aviation or security experience required - a walkthrough guide is provided for beginners, and volunteers are on hand to help at every step. This activity is accessible to all skill levels.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Aerospace Village - Sunday - 10:00-13:59 PDT

Title: Bricks in the Air

Tags: Aerospace Village | Creator Event/Activity

When: Sunday, Aug 9, 10:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 2 700 (Aerospace Village) - [Map](#)

Description:

Step right up to our interactive LEGO aircraft. Can you investigate the aircraft's control system, identify any vulnerabilities, and “hack” beyond its intended functions?

This exercise uses real-world I2C protocols to simulate potential vulnerabilities in an aircraft control system.

No specialized hardware required - all target devices, materials, and interfaces are provided!

No prior aviation or security experience required - a walkthrough guide is provided for beginners, and volunteers are on hand to help at every step. This activity is accessible to all skill levels.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Aerospace Village - Saturday - 10:00-17:59 PDT

Title: Bricks in the Air

Tags: Aerospace Village | Creator Event/Activity

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 2 700 (Aerospace Village) - [Map](#)

Description:

Step right up to our interactive LEGO aircraft. Can you investigate the aircraft's control system, identify any vulnerabilities, and “hack” beyond its intended functions?

This exercise uses real-world I2C protocols to simulate potential vulnerabilities in an aircraft control system.

No specialized hardware required - all target devices, materials, and interfaces are provided!

No prior aviation or security experience required - a walkthrough guide is provided for beginners, and volunteers are on hand to help at every step. This activity is accessible to all skill levels.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

DEF CON Training - Tuesday - 08:30-17:30 PDT

Title: Bridging the GAP: Hands-On Embedded Hardware Hacking

Tags: DEF CON Training (Paid) (2-day) | DEF CON Training

When: Tuesday, Aug 11, 08:30 - 17:30 PDT

Where: LVCCW Level 2 W238 (DEF CON Groups) - [Map](#)

Description:

Speakers: Aaron Wasserman, Garrett Freibott, Will McCardell

SpeakerBio: Aaron Wasserman, Praetorian

No BIO available

SpeakerBio: Garrett Freibott, Praetorian

No BIO available

SpeakerBio: Will McCardell, Praetorian

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

DEF CON Training - Monday - 08:30-17:30 PDT

Title: Bridging the GAP: Hands-On Embedded Hardware Hacking

Tags: DEF CON Training (Paid) (2-day) | DEF CON Training

When: Monday, Aug 10, 08:30 - 17:30 PDT

Where: LVCCW Level 2 W238 (DEF CON Groups) - [Map](#)

Description:

Speakers: Aaron Wasserman, Garrett Freibott, Will McCardell

SpeakerBio: Aaron Wasserman, Praetorian

No BIO available

SpeakerBio: Garrett Freibott, Praetorian

No BIO available

SpeakerBio: Will McCardell, Praetorian

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Bring Your Own Root Of Trust

Tags: DEF CON Official Talk | Demo | Tool | Exploit

When: Saturday, Aug 8, 13:30 - 14:30 PDT

Where: LVCCW Level 1 Hall 3 1007 (Main Track 2) - [Map](#)

Description:

Modern computers depend on a hardware root of trust: a component assumed to start trustworthy and is used to verify everything that follows. This has evolved from ROM boot code and fixed keys into TPMs, secure boot chains, external security controllers, and attestation mechanisms used far beyond disk encryption. Today, platforms trust these devices because they are certified, immutable, and built into the hardware, but what if that assumption is wrong? Starting from real hardware traces, failed approaches, and a pile of development boards, we arrive at a \$45 FPGA-based SPI TPM that can appear to Windows 11 as a platform trust anchor. From there, we explore what this means for secure boot, measured boot, platform attestation, anticheat, AI infrastructure, and the broader belief that hardware identity is difficult to counterfeit. We will release the code, gateway, prompts, and data so others can reproduce the work and push it further.

<https://twpm.dasharo.com/> <https://github.com/microsoft/ms-tpm-20-ref>

Speakers: Mickey "@HackingThings" Shkatov, Jesse Michael

SpeakerBio: Mickey "@HackingThings" Shkatov, Eclipsium

Mickey has been involved in security research for over a decade, specializing in breaking down complex concepts and identifying security vulnerabilities in unusual places. His experience spans a variety of topics, which he has presented at security conferences worldwide. His talks have covered areas ranging from web penetration testing to the intricacies of BIOS firmware.

SpeakerBio: Jesse Michael, Eclipsium

Jesse is an experienced security researcher focused on vulnerability detection and mitigation who has worked at all layers of modern computing environments from exploiting worldwide corporate network infrastructure down to hunting vulnerabilities inside processors at the hardware design level. His primary areas of expertise include reverse engineering embedded firmware and exploit development. He has also presented research at DEF CON, Black Hat, PacSec, Hackito Ergo Sum, Ekoparty, and BSides Portland.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Bring-Your-Own-EDR - Breaking Windows Process Protection to build EDR-Protected Malware

Tags: DEF CON Official Talk | Demo | Tool | Exploit

When: Friday, Aug 7, 13:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 3 906 (Main Track 3) - [Map](#)

Description:

The core assumption of modern endpoint defense is broken. While Endpoint Detection and Response (EDR) solutions are built to restrict administrators through Protected Process Light (PPL) and anti-tampering, this research reveals an industry-wide design flaw: the "Bring-Your-Own-EDR" (BYOEDR) technique. We demonstrate a post-exploitation scenario where a local administrator weaponizes the EDR's own trusted installer to bypass its formidable defenses, establishing a self-protected malware. This shows a structural weakness in how security products handle installation and trust. We will show a complete exploit chain that any attacker can leverage to achieve arbitrary unsigned code execution within PPL boundaries.

Ultimately, the strongest defender becomes the attacker's most powerful tool.

<https://blog.slowerzs.net/posts/pplsystem/> https://github.com/hasherezade/pe_to_shellcode/
<https://github.com/googleprojectzero/symboliclink-testing-tools>

SpeakerBio: Shahak Morag, Akamai

Shahak Morag is currently serving as the Senior Security Researcher at Akamai, with more than seven years of experience in security research. His background includes extensive expertise in Linux kernel, embedded systems, and Windows internals.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Bruce's Fireside Chat

Tags: AI Village | Creator Talk/Panel

When: Friday, Aug 7, 16:00 - 16:59 PDT

Where: LVCCW Level 1 Hall 2 603 (AI Village) - [Map](#)

Description:

This is a sit down discussion in a more casual conversational format: Topic TBA

SpeakerBio: Bruce Schneier, Advisory Board Member at VerifiedVoting.org

Bruce Schneier is an internationally renowned security technologist, called a “security guru” by the Economist. He is the New York Times best-selling author of 14 books – including *Rewiring Democracy* and *A Hacker’s Mind* -- as well as hundreds of articles, essays, and academic papers. His long-running newsletter and blog, “Schneier on Security,” is one of the most popular sources of cybersecurity news on the internet. Schneier is a Fellow and Lecturer in Public Policy at the Harvard Kennedy School and the Munk School at the University of Toronto. He is a fellow at the Berkman-Klein Center for Internet and Society at Harvard University, a board member of the Electronic Frontier Foundation and AccessNow, and an advisory board member of EPIC and VerifiedVoting.org. He is also the Chief of Security Architecture at Inrupt, Inc.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: BTR Reforged: Weaponizing Defender's Remediation Driver as a Kernel Operation Primitive

Tags: DEF CON Official Talk | Demo | Tool

When: Friday, Aug 7, 12:30 - 13:30 PDT

Where: LVCCW Level 1 Hall 3 1007 (Main Track 2) - [Map](#)

Description:

What if a trusted security component could be repurposed into an attacker-controlled kernel primitive? What if a signed Microsoft remediation driver could be instructed to execute arbitrary file and registry operations from Ring 0 — without exploits, vulnerabilities, or memory corruption?

In this talk, we present the first full reverse engineering of the Windows Defender Boot-Time Removal driver (BTR.sys) and its proprietary transaction format. We dissect its encrypted configuration mechanism, integrity validation logic, and execution pipeline, and demonstrate how this legitimate remediation component can be transformed into a universal kernel operation engine. We introduce BTR_CLI, a research tool that constructs valid encrypted transactions and exercises the driver's capabilities.

We demonstrate how BTR_CLI can be used as an EDR/AV bypass technique, disarming security solutions using a trusted Windows built-in, Microsoft-signed driver — without relying on typical BYOVD techniques.

Our research reveals how trusted security infrastructure can unintentionally expose powerful primitives and what this means for defenders. This talk blends reverse engineering, kernel internals, and detection engineering into a practical case study of when defensive technology becomes offensive capability.

SpeakerBio: Jiří Vinopal, Threat Researcher at Check Point Research

Jiří Vinopal is a security researcher, malware researcher, and reverse engineer at Check Point Research, focused on advanced cyber threats, kernel internals, and the hidden mechanics of undocumented system components. His work spans uncovering novel attack primitives, reconstructing proprietary protocols from binary analysis alone, and deep-diving into both sophisticated malware families and trusted platform components. When he's not buried in disassembly, he actively shares his knowledge and passion for reverse engineering across his X account, YouTube channel, and blog — delivering tips, tricks, and technical insights to fellow enthusiasts and the broader security community.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Bug Bounty Village - Sunday - 13:45-14:15 PDT

Title: Bug Bounty Village Closing Ceremony

Tags: Bug Bounty Village | Creator Talk/Panel

When: Sunday, Aug 9, 13:45 - 14:15 PDT

Where: LVCCW Level 2 W206-207 (Bug Bounty Village) - [Map](#)

Description:

Final words, thanks, and giveaways.

SpeakerBio: Bug Bounty Village Staff

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Contests - Saturday - 10:00-10:59 PDT

Title: Bug Bounty Village CTF - Open

Tags: Bug Bounty Village | Bug Bounty Village CTF | Contest

When: Saturday, Aug 8, 10:00 - 10:59 PDT

Where: Online

Description:



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Contests - Friday - 10:00-10:59 PDT

Title: Bug Bounty Village CTF - Open

Tags: Bug Bounty Village | Bug Bounty Village CTF | Contest

When: Friday, Aug 7, 10:00 - 10:59 PDT

Where: Online

Description:



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Contests - Sunday - 13:00-13:45 PDT

Title: Bug Bounty Village CTF Awards

Tags: Bug Bounty Village | Bug Bounty Village CTF | Contest

When: Sunday, Aug 9, 13:00 - 13:45 PDT

Where: LVCCW Level 2 W206-207 (Bug Bounty Village) - [Map](#)

Description:

Join us at the Bug Bounty Village for the CTF Award Ceremony, where we celebrate the top performers of our inaugural Capture The Flag competition. During this in-person ceremony, we'll recognize the highest-ranking participants on the leaderboard and award prizes to those present. If you've competed in the CTF and secured a spot on the leaderboard, make sure to attend and claim your prize! This is a unique opportunity to honor the skill and creativity of the global hacking community and to connect with fellow researchers and organizers. We look forward to seeing you there!

SpeakerBio: Bug Bounty Village Staff

No BIO available

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

The Diana Initiative - Friday - 13:40-13:50 PDT

Title: Bug Bounty Village Tour

Tags: The Diana Initiative | Creator Tour

When: Friday, Aug 7, 13:40 - 13:50 PDT

Where: LVCCW Level 1 South Lobby / Atrium - [Map](#)

Description:

Interested in visiting Bug Bounty Village but afraid to go by yourself? The Diana Initiative is hosting tours! Follow a volunteer to Bug Bounty Village and be introduced to the community and activities inside!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

IoT Village - Friday - 12:00-13:30 PDT

Title: Build Your Own Meshtastic Node: Off-Grid, Encrypted LoRa Meshnets for Beginners!

Tags: IoT Village | Creator Workshop

When: Friday, Aug 7, 12:00 - 13:30 PDT

Where: LVCCW Level 1 Hall 1 215 (IoT Village) - [Map](#)

Description:

Beginners can now create off-grid, encrypted mesh networks for cheap, with applications in emergency communication, sensor monitoring, and more! Kit Cost: \$80. Class Cap: 30.

SpeakerBio: Kody Kinzie

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Build-A-Badge Workshop

Tags: Maker's Village | Creator Event/Activity

When: Saturday, Aug 8, 11:00 - 12:30 PDT

Where: LVCCW Level 1 Hall 1 301 (Makers' Village) - [Map](#)

Description:

Welcome to the Build-A-Badge Workshop! We've cultivated some interesting maker mediums to bring you a unique badge that's all about making it your own. This workshop is a unique experience for the veteran maker or someone new that may be interested in seeing how makers can come together and create something truly unique. A brief workshop introduction, led by project leader and designer Alchemist, will give you some background on the badge. After which, you'll be assigned a group number and split off into teams within the Makers' Village, hitting each station for the badge assembly. You'll get a chance to talk to our 3-D printer Buddha, our Laser Engraver Teazee, Silk Screener hunny, and Board Maker M-Nelly to show you all the ways you can make this Bear Badge your own. Every workshop attendee will also receive a SAO for their badges as well as stickers and links to a Badge Repository with prints files, patterns, and some extras to continue to work on this badge after the con.

Speakers: hunny, Teazee, Buddha, MLP, M-Nelly, Alchemmer

SpeakerBio: hunny

No BIO available

SpeakerBio: Teazee

No BIO available

SpeakerBio: Buddha

No BIO available

SpeakerBio: MLP

No BIO available

SpeakerBio: M-Nelly

No BIO available

SpeakerBio: Alchemmer

No BIO available

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Build-A-Badge Workshop

Tags: Maker's Village | Creator Event/Activity

When: Friday, Aug 7, 11:00 - 12:30 PDT

Where: LVCCW Level 1 Hall 1 301 (Makers' Village) - [Map](#)

Description:

Welcome to the Build-A-Badge Workshop! We've cultivated some interesting maker mediums to bring you a unique badge that's all about making it your own. This workshop is a unique experience for the veteran maker or someone new that may be interested in seeing how makers can come together and create something truly unique. A brief workshop introduction, led by project leader and designer Alchemist, will give you some background on the badge. After which, you'll be assigned a group number and split off into teams within the Makers' Village, hitting each station for the badge assembly. You'll get a chance to talk to our 3-D printer Buddha, our Laser Engraver Teazee, Silk Screener hunny, and Board Maker M-Nelly to show you all the ways you can make this Bear Badge your own. Every workshop attendee will also receive a SAO for their badges as well as stickers and links to a Badge Repository with prints files, patterns, and some extras to continue to work on this badge after the con.

Speakers: hunny, Teazee, Buddha, MLP, M-Nelly, Alchemmer

SpeakerBio: hunny

No BIO available

SpeakerBio: Teazee

No BIO available

SpeakerBio: Buddha

No BIO available

SpeakerBio: MLP

No BIO available

SpeakerBio: M-Nelly

No BIO available

SpeakerBio: Alchemmer

No BIO available

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Build-A-Badge Workshop

Tags: Maker's Village | Creator Event/Activity

When: Friday, Aug 7, 14:00 - 15:30 PDT

Where: LVCCW Level 1 Hall 1 301 (Makers' Village) - [Map](#)

Description:

Welcome to the Build-A-Badge Workshop! We've cultivated some interesting maker mediums to bring you a unique badge that's all about making it your own. This workshop is a unique experience for the veteran maker or someone new that may be interested in seeing how makers can come together and create something truly unique. A brief workshop introduction, led by project leader and designer Alchemist, will give you some background on the badge. After which, you'll be assigned a group number and split off into teams within the Makers' Village, hitting each station for the badge assembly. You'll get a chance to talk to our 3-D printer Buddha, our Laser Engraver Teazee, Silk Screener hunny, and Board Maker M-Nelly to show you all the ways you can make this Bear Badge your own. Every workshop attendee will also receive a SAO for their badges as well as stickers and links to a Badge Repository with prints files, patterns, and some extras to continue to work on this badge after the con.

Speakers: hunny, Teazee, Buddha, MLP, M-Nelly, Alchemmer

SpeakerBio: hunny

No BIO available

SpeakerBio: Teazee

No BIO available

SpeakerBio: Buddha

No BIO available

SpeakerBio: MLP

No BIO available

SpeakerBio: M-Nelly

No BIO available

SpeakerBio: Alchemmer

No BIO available

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Building a Hacker Haven: The Long Game of Growing a Local Hacker Community

Tags: DEF CON Groups | Creator Talk/Panel

When: Saturday, Aug 8, 11:00 - 11:30 PDT

Where: LVCCW Level 1 Hall 3 1100 (Creator Stage 7) - [Map](#)

Description:

DEF CON 30 sent us home with an idea: our city needed a hacker community.

Three years later, that idea has grown into a 501(c)(3) nonprofit, a thriving monthly meetup, a network that helped us launch a regional conference (wiscon.io), and a long-term vision for a brick-and-mortar hackerspace. Along the way, we've learned a lot, made our share of mistakes, and discovered what it really takes to build a sustainable community from the ground up.

This talk is a practical guide to starting and growing a DEF CON Group without burning yourself out in the process. We'll cover getting approved by DEF CON Groups, incorporating as a nonprofit, raising money from your community, building a board that works well together, writing bylaws that set you up for success, handling Code of Conduct issues, and planning for long-term growth beyond monthly meetups.

We'll also talk about something that doesn't get enough attention, building a community as a team. The strongest groups aren't built by one person doing everything, they're built by people who share the workload, support one another, and create something that can outlast any single organizer.

Expect honest lessons learned, practical advice, real numbers, and plenty of war stories. We'll also provide a companion website packed with all the details that you can adapt for your own community.

If you've ever thought about starting a DEF CON Group, building a local hacker community, or creating something that brings people together, this talk is for you!

Speakers: Ryan Zagrodnik, Allie Zagrodnik

SpeakerBio: Ryan Zagrodnik, DC608

Ryan Zagrodnik is a Senior Penetration Tester with over sixteen years of experience in offensive and defensive security roles. He holds OSCP and CISSP certifications and has previously worked on internal red teams and held a U.S. Government security clearance doing offensive security for the Department of Defense and Department of Education. Ryan has presented at CypherCon, SecretCon, DEF CON Hardware Hacking Village, BSides MKE, GRASSr00tz, and Skunks Misery.

SpeakerBio: Allie Zagrodnik, DC608

Allie Zagrodnik is a cybersecurity professional and community organizer based in Madison, Wisconsin and quickly discovered a passion for the human side of security, community building, and mentorship within the industry.

She is the cofounder of DC608, a Madison-based DEF CON group focused on creating an inclusive and welcoming space for anyone interested in cybersecurity, regardless of skill level or background. She is also the founder of Wisconsin Information Security Conference, a community-driven conference focused on education, networking, and growing the cybersecurity community throughout the Midwest.

Outside of cybersecurity, Allie enjoys spending time with her husband, three dogs, and three cats, while proudly representing Wisconsin through her love of the Green Bay Packers and the local hacker community.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Building a State Wide VDP: Lessons from Maryland's First Year in the Trenches

Tags: Policy @ DEF CON | Creator Talk/Panel

When: Friday, Aug 7, 16:00 - 16:30 PDT

Where: LVCCW Level 1 Hall 3 1103 (Creator Stage 5) - [Map](#)

Description:

State and local governments are soft targets. Smaller security teams, legacy infrastructure, high-value data, and tight budgets make them attractive to adversaries. Yet most lack basic proactive security programs like Vulnerability Disclosure Programs (VDPs). In January 2025, I was hired as Maryland's first Adversary Emulation Manager and tasked with standing up a statewide VDP. Coming from DoD cyber operations but new to the bug bounty space, I had to figure out how to build a program that would actually work, not just check a compliance box. The result: Maryland's VDP launched in October 2025 and has been a success because we fought for true safe harbor, assumed noble intent, and took a researcher-first approach. This talk shares what I learned building the program from scratch. I'll cover the hard conversations with legal teams who feared "authorizing hacking," the fights for wide scope instead of narrow carve-outs, and why safe harbor isn't optional. If you're a state or local practitioner, you'll walk away with a replication guide. If you're a policymaker, you'll understand why VDPs matter. If you're a researcher, you'll see what makes programs succeed or fail.

SpeakerBio: 01dbae

01dbae has worked in technology since the early 2000s, spanning data center operations, private cloud computing, and information security. After moving into security at a large publisher, he transitioned into government contracting and later served as a DoD civilian supporting the cyber counterintelligence mission. He also spent a few seasons with the Baltimore Ravens.

01dbae later joined the State of Maryland as Adversary Emulation Manager, tasked with standing up the state's first Vulnerability Disclosure Program — despite having never run a bug bounty program before. That outsider perspective helped him challenge assumptions and push for researcher-first policies over compliance theater. The program launched with strong safe harbor protections and broad scope, and has been running successfully since. There are lessons in that process worth sharing with other state and local governments building proactive security programs

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

DEF CON Groups - Saturday - 13:00-13:30 PDT

Title: Building a Strong Community Culture presented by DC407

Tags: DEF CON Groups | Creator Talk/Panel

When: Saturday, Aug 8, 13:00 - 13:30 PDT

Where: LVCCW Level 1 Hall 3 1100 (Creator Stage 7) - [Map](#)

Description:

Healthy DEF CON Groups are built by more than one person. This session focuses on creating a community culture where members are encouraged to participate, contribute, speak, volunteer, and eventually help lead. DC407 will discuss consistency, mentorship, leadership mindset, and practical ways to move people from passive attendance into active involvement. This workshop is for organizers who want to build a group that is welcoming, resilient, and bigger than any single organizer.

Speakers:Edna Jonsson,Dustin

SpeakerBio: Edna Jonsson, DC407

Edna is one of the DC407 group leaders and enjoys helping others come up in the cyber community. Edna is the volunteer coordinator at BSides Orlando and hosts the Security Chipmunks podcast.

SpeakerBio: Dustin, DC407

I enjoy helping people. I'm a security enthusiast, if it's related to security then I'm probably interested. I've helped facilitate DC47 for 8+ years.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Building a Student-Led OSINT Program to Investigate Cryptocurrency Fraud

Tags: OSINT For Good Community | Creator Talk/Panel

When: Sunday, Aug 9, 13:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 4 1307 (OSINT4Good Community) Stage - [Map](#)

Description:

ScamBusters is a student-facing OSINT investigation program that trains students to identify, trace, and report cryptocurrency fraud infrastructure — from pig-butcher scam domains to the wallet networks behind them. This talk shares how the program works, what students have actually found (hundreds of scam domains and wallet clusters tied to organized fraud rings), and how the reporting pipeline connects student research to real-world action.

SpeakerBio: Angela Ramos, University of Tampa

Angela Ramos is a University of Tampa cybersecurity lecturer. She leads the Scam Busters student program, coaches Trace Labs Search Party CTFs, and volunteers with US Cyber Games. She holds the GCIH, GSLC, and CEH certifications and spent a decade in DoD cyber operations.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Lockpick Village - Friday - 11:00-11:59 PDT

Title: Building an open source safecracking robot

Tags: Lockpick Village | Creator Talk/Panel

When: Friday, Aug 7, 11:00 - 11:59 PDT

Where: LVCCW Level 1 Hall 1 407 (Lockpick Village) - [Map](#)

Description:

An auto dialer is a device that brute forces the combination to a safe lock. These often start in the thousands of dollars when it's only a motor that spins. This talk will cover how safe locks work, what goes into building one of these devices, and all the resources (including the source code) for making your own for cheap.

SpeakerBio: Jared Dygert

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Building Better Backdoors Than China

Tags: Packet Hacking Village | Creator Talk/Panel

When: Saturday, Aug 8, 13:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 3 1102 (Creator Stage 6) - [Map](#)

Description:

PhantomShell is a Linux command & control implant that sniffs traffic of active TCP services to create a bidirectional C2 channel through any open port, using only stateful inbound traffic. It captures packets at the link layer, allowing it to read packets destined for legitimate services. Responses are constructed as raw TCP frames with sequence numbers derived from the original connection, making them difficult to distinguish from the service's own replies. This effectively turns every open service port into a bind shell, making the implant effectively impossible to firewall so long as any service remains externally accessible.

SpeakerBio: Khael Kugler, Lead Offensive Security Engineer, Praetorian Security, Inc.

Khael Kugler is a Lead Security Engineer at Praetorian, where he primarily executes on red team and IoT engagements. Khael also volunteers as a red teamer for multiple CCDC regions, primarily focusing on linux persistence for SECCDC and WRCCDC (if you're interested in helping, reach out!).

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Hackers.town - Friday - 11:00-11:59 PDT

Title: building community and privacy tools from junk

Tags: Hackers.town | Creator Talk/Panel

When: Friday, Aug 7, 11:00 - 11:59 PDT

Where: LVCCW Level 1 Hall 4 1420 (Hackers.town) - [Map](#)

Description:

SpeakerBio: TheGibson

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Building Hackbots

Tags: Recon Village | Creator Talk/Panel

When: Sunday, Aug 9, 12:30 - 12:59 PDT

Where: LVCCW Level 1 Hall 3 1103 (Creator Stage 5) - [Map](#)

Description:

Building AI-Powered Penetration Testing Bots In this talk, we'll walk through the core design philosophy behind AI hackbots and the architecture that makes them work: single-purpose vs. multi-stage bots, context engineering for targeted prompting, and tool integration with output parsing workflows. Then we'll get hands-on. We'll live-build a functional hackbot for a common offensive task — demonstrating asset discovery, endpoint analysis, or mutation-focused testing (e.g., XSS/SSRF) — and show how context engineering and hallucination mitigation work in practice against real targets. You'll see where AI genuinely accelerates reconnaissance and web analysis, and where it falls flat if you aren't careful. We'll close with lessons on cost optimization, auditability, and integrating hackbots into actual engagements. Who should attend: Pentesters and bug bounty hunters with offensive security experience who want to meaningfully integrate AI into their workflow — not as a novelty, but as reliable tooling. What you'll walk away with: A clear mental model for when and how to build hackbots, a live demo you can replicate, and a path into the full course where you'll build seven production-ready bots from asset discovery through mutation testing.

SpeakerBio: Jason "jhaddix" Haddix, CEO and "Hacker in Charge" at Arcanum Information Security

Jason Haddix AKA jhaddix is the CEO and “Hacker in Charge” at Arcanum Information Security. Arcanum is a world class assessment and training company.

Jason has had a distinguished 20-year career in cybersecurity previously serving as CISO of FLARE, CISO of Buddobot, CISO of Ubisoft, Head of Trust/Security/Operations at Bugcrowd, Director of Penetration Testing at HP, and Lead Penetration Tester at Redspin. He has also held positions doing mobile penetration testing, network/infrastructure security assessments, and static analysis. Jason is a hacker, bug hunter and currently ranked 57th all-time on Bugcrowd's bug bounty leaderboards. Currently, he specializes in recon, web application analysis, and emerging technologies. Jason has also authored many talks on offensive security methodology, including speaking at cons such as DEFCON, Bsides, BlackHat, RSA, OWASP, Nullcon, SANS, IANS, BruCon, Toorcon and many more.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Building Hackbots

Tags: AppSec Village | Creator Talk/Panel | All Audiences

When: Saturday, Aug 8, 10:30 - 10:59 PDT

Where: LVCCW Level 1 Hall 2 604 (Appsec Village) Main Stage - [Map](#)

Description:

Building AI-Powered Penetration Testing Bots

SpeakerBio: Jason "jhaddix" Haddix, CEO and "Hacker in Charge" at Arcanum Information Security

Jason Haddix AKA jhaddix is the CEO and “Hacker in Charge” at Arcanum Information Security. Arcanum is a world class assessment and training company.

Jason has had a distinguished 20-year career in cybersecurity previously serving as CISO of FLARE, CISO of Buddobot, CISO of Ubisoft, Head of Trust/Security/Operations at Bugcrowd, Director of Penetration Testing at HP, and Lead Penetration Tester at Redspin. He has also held positions doing mobile penetration testing, network/infrastructure security assessments, and static analysis. Jason is a hacker, bug hunter and currently ranked 57th all-time on Bugcrowd’s bug bounty leaderboards. Currently, he specializes in recon, web application analysis, and emerging technologies. Jason has also authored many talks on offensive security methodology, including speaking at cons such as DEFCON, Bsides, BlackHat, RSA, OWASP, Nullcon, SANS, IANS, BruCon, Toorcon and many more.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Building Hackbots

Tags: Red Team Village | Misc

When: Saturday, Aug 8, 12:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 1 309 (Red Team Village) Tactic Table 3 - [Map](#)

Description:

Description: Building AI-Powered Penetration Testing Bots

In this talk, we'll walk through the core design philosophy behind AI hackbots and the architecture that makes them work: single-purpose vs. multi-stage bots, context engineering for targeted prompting, and tool integration with output parsing workflows.

Then we'll get hands-on. We'll live-build a functional hackbot for a common offensive task — demonstrating asset discovery, endpoint analysis, or mutation-focused testing (e.g., XSS/SSRF) — and show how context engineering and hallucination mitigation work in practice against real targets. You'll see where AI genuinely accelerates reconnaissance and web analysis, and where it falls flat if you aren't careful. We'll close with lessons on cost optimization, auditability, and integrating hackbots into actual engagements.

Who should attend: Pentesters and bug bounty hunters with offensive security experience who want to meaningfully integrate AI into their workflow — not as a novelty, but as reliable tooling.

What you'll walk away with: A clear mental model for when and how to build hackbots, a live demo you can replicate, and a path into the full course where you'll build seven production-ready bots from asset discovery through mutation testing.

Speakers: Jason "jhaddix" Haddix, Ryan Bonner

SpeakerBio: Jason "jhaddix" Haddix, CEO and "Hacker in Charge" at Arcanum Information Security

Jason Haddix AKA jhaddix is the CEO and “Hacker in Charge” at Arcanum Information Security. Arcanum is a world class assessment and training company.

Jason has had a distinguished 20-year career in cybersecurity previously serving as CISO of FLARE, CISO of Buddobot, CISO of Ubisoft, Head of Trust/Security/Operations at Bugcrowd, Director of Penetration Testing at HP, and Lead Penetration Tester at Redspin. He has also held positions doing mobile penetration testing, network/infrastructure security assessments, and static analysis. Jason is a hacker, bug hunter and currently ranked 57th all-time on Bugcrowd's bug bounty leaderboards. Currently, he specializes in recon, web application analysis, and emerging technologies. Jason has also authored many talks on offensive security methodology, including speaking at cons such as DEFCON, Bsides, BlackHat, RSA, OWASP, Nullcon, SANS, IANS, BruCon, Toorcon and many more.

SpeakerBio: Ryan Bonner, Lead Security Engineer at Arcanum Information Security

Ryan Bonner is a Lead Security Engineer at Arcanum Information Security, where he builds AI systems, hacks them, and runs application penetration tests. Off the clock he hunts wide-scope bug bounty programs.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Building Project Obsidian: Designing the Blue Team CTF for DEF CON

Tags: Blue Team Village | Creator Talk/Panel

When: Friday, Aug 7, 14:30 - 15:30 PDT

Where: LVCCW Level 2 W217 (Blue Team Village) Main Stage - [Map](#)

Description:

What does it take to build a realistic blue team training platform for thousands of DEF CON attendees? Join the engineers behind Project Obsidian as we discuss the architecture, design decisions, and lessons learned while building a cloud-native incident response and malware analysis CTF. We'll cover Kubernetes, automation, AI-assisted challenge creation, scalable infrastructure, and the balance between realism and accessibility. Whether you're interested in CTF design, defensive security, or modern platform engineering, this panel offers an inside look at how a community-driven project comes together.

Speakers: Carlo Anez Mazurco, Chris "dafinga" Maenner, Omenscan ~, Paul Goffar

SpeakerBio: Carlo Anez Mazurco

Carlo Anez Mazurco is a cybersecurity instructor, consultant, and community leader with more than 15 years of experience across security operations, threat intelligence, incident response, threat hunting, and detection engineering. He is the Founder of IgniteCyber Academy, a DEF CON Training instructor, and an active contributor to Blue Team Village, where he supports Project Obsidian and develops hands-on blue team content for the cybersecurity community.

Carlo specializes in helping defenders translate attacker tradecraft into practical detection and response techniques while responsibly integrating artificial intelligence into modern security operations. His work focuses on creating realistic labs, CTF challenges, and immersive training environments that prepare students for real-world investigations using enterprise telemetry, cloud technologies, and AI-assisted workflows.

He has delivered training and presentations for conferences, universities, government organizations, and commercial teams, with a passion for mentoring the next generation of cybersecurity professionals. His goal is to make complex security concepts approachable through practical demonstrations, collaborative learning, and hands-on exercises that participants can immediately apply in their own environments.

SpeakerBio: Chris "dafinga" Maenner, Board Member at BSides Philadelphia

Chris Maenner is the founder of Palmtree Ventures, where he spends his time securing AI systems, Kubernetes, cloud platforms, and developer tooling without getting in the way of shipping software. Over the last 15+ years, he's worked across startups and Fortune 50 companies building product, platform, and cloud security programs. When he's not doing his day job, Chris helps build CTFs and security projects for DEF CON's Blue Team Village and OWASP, including leading engineering efforts around Project Obsidian. He also serves on the board of BSides Philadelphia, contributes to the OWASP Secure Agent Playbook, and regularly speaks about AI security, Kubernetes, cloud-native security, and the lessons learned from actually trying to secure this stuff in production.

SpeakerBio: Omenscan ~

Some people write books to document and share what they learn. I write software. @Blueteamvillage Director. I do not speak for my employer, their clients, or customers

SpeakerBio: Paul Goffar

Paul Goffar is the founder of Raven Cybersecurity, doing offensive and defensive security consulting for small and mid-sized businesses. Day to day, he runs incident response, detection engineering, digital forensics, and threat intelligence for an enterprise SOC in the automotive sector.

For the last five years, Paul has worked closely with Blue Team Village as an engineering lead for competitions and content delivery around the US, and does similar CTF and content work with CTF313, a Detroit-based team. He holds several industry certifications including GCIH, GMON, GNFA, CRTP, and paWASP. A father of three, a Metro Detroit native, and a hacker at heart, he continuously finds ways to give back to the community through mentoring and extensive volunteer work.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Maker's Village - Saturday - 16:00-17:45 PDT

Title: Building Silkscreens and carving stamps

Tags: Maker's Village | Creator Event/Activity

When: Saturday, Aug 8, 16:00 - 17:45 PDT

Where: LVCCW Level 1 Hall 1 301 (Makers' Village) - [Map](#)

Description:

See a demonstration of the steps to making your own silk screens and get to explore the Makers' Village Stamps and screens. Bring swag to experiment on!

SpeakerBio: hunny

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Maritime Hacking Village - Friday - 11:30-12:15 PDT

Title: Building the Humans Behind the Mission: Talent, Readiness, and Cyber Power for America's Armed Services

Tags: Maritime Hacking Village | Creator Talk/Panel

When: Friday, Aug 7, 11:30 - 12:15 PDT

Where: LVCCW Level 1 Hall 3 801 (Creator Stage 2) - [Map](#)

Description:

The Maritime Hacking Village is proud to host a first of its kind conversation with the Principal Cyber Advisors to the Navy and the Air Force. As cyber operations become inseparable from maritime, air, and joint missions, the Navy and Air Force face a shared challenge: how to recruit, train, integrate, and retain the technical talent required for modern conflict.

This session will explore how the services are strengthening operational cyber units. How deeply technical experts can be woven into traditional command structures, and how joint missions can be supported by interoperable training pipelines. We'll also dig into the realities of competing with the commercial sector for high end cyber talent, and the emerging skill sets — from AI engineering to cloud and data center operations — that will define future conflict. Expect a little honesty, and maybe one or two jokes about how retention would be easier if the military offered free energy drinks and a hoodie.

Speakers: Dr. Nina Kollars, Dr. Wanda T. Jones-Heath, Anne Marie Schumann

SpeakerBio: Dr. Nina Kollars, US Naval War College

Dr. Nina Kollars is an Associate Professor at the U.S. Naval War College's Cyber and Innovation Policy Institute, where she specializes in cyber resilience, emerging technologies, and wargaming efforts focused on Taiwan and the Pacific. Dr. Kollars also serves as co-director of the Maritime Hacking Village, a 501c3 that advances ethical hacking on maritime assets and infrastructure. She is also an executive bourbon steward.

SpeakerBio: Dr. Wanda T. Jones-Heath, Principal Cyber Advisor for the Department of the Air Force

Dr. Wanda T. Jones-Heath, a member of the Senior Executive Service, is the Principal Cyber Advisor for the Department of the Air Force, comprised of the U.S. Air Force and U.S. Space Force. As the Principal Cyber Advisor for the DAF, her duties include synchronizing, coordinating and overseeing the implementation of the DAF Cyber Strategy and advising the Secretary of the Air Force on all cyber programs. She is responsible for overseeing cyberspace recruitment; resourcing and training of cyber mission forces, as well as assessing their readiness; overseeing acquisition; advocate for cyber investments; cybersecurity supply chain risk management; security of information systems and weapon systems.

SpeakerBio: Anne Marie Schumann, Principal Cyber Advisor, Department of the Navy

Ms. Anne Marie Schumann serves as the Department of the Navy Principal Cyber Advisor (DON PCA). In this role, she is responsible for advising the Secretary of the Navy, Chief of Naval Operations, and Commandant of the Marine Corps on all cyber matters and implementing the Department of Defense Cyber Strategy within the DON.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Noob Community - Friday - 16:00-16:30 PDT

Title: Building Your First Homelab

Tags: Noob Community | Creator Talk/Panel

When: Friday, Aug 7, 16:00 - 16:30 PDT

Where: LVCCW Level 1 Hall 4 1417 (Noob Community) - [Map](#)

Description:

Have you wanted to build a homelab but felt overwhelmed by all the choices? This talk is for you. Building a homelab doesn't have to be complex or intimidating, I'll walk you through how easy and simple it can be to set up your first lab and get hands on experience with popular cybersecurity and IT tools.

SpeakerBio: Stephen Glombicki

No BIO available

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Burning Redirectors Before Blue Team Does

Tags: Red Team Village | Misc

When: Friday, Aug 7, 12:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 1 309 (Red Team Village) Tactic Table 1 - [Map](#)

Description:

Red team operators rely on redirectors to proxy C2 callbacks, but monitoring those redirectors for blue team detection is typically handled by either manual log review or deploying a full SIEM pipeline. Neither scales well during active assessments. NightWatcher is a traffic monitoring agent that analyzes redirector access logs through detection rules and a reasoning engine that identifies attack phase progression (reconnaissance through takedown) rather than issuing disconnected alerts. NightRouter is a decision routing agent that receives NightWatcher's assessments, recommends a redirector action (drain, reduce weight, quarantine), and presents it to the operator via Slack interactive messages for approval or rejection.

In this tactic, attendees will deploy NightWatcher/NightRouter locally, simulate blue team traffic patterns against redirectors, observe the attack phase reasoning and escalation detection, and execute redirector actions through the Slack human-in-the-loop approval flow. The stack runs in mock mode with no external infrastructure dependencies required.

Speakers: Mohamed AbuMuslim, Saad Nasir

SpeakerBio: Mohamed AbuMuslim

I am a security researcher and offensive security engineer specializing in red teaming, penetration testing, adversarial AI, and product security engineering.

My work focuses on identifying exploitable weaknesses across modern attack surfaces, including web applications, APIs, cloud platforms, enterprise infrastructure, Active Directory, and LLM-enabled systems. I combine offensive operations, applied research, and security engineering to solve complex security problems, validate security posture, and improve how organizations build and assess secure products.

Over the years, I have led and contributed to offensive security capability building in complex environments, including helping establish Microsoft Egypt & Middle East's first offensive security team and previously helping build PwC's offensive security capability in Egypt, and served as Manager and Practice Lead at EY leading offensive security engagements. My experience spans startups, mid-sized organizations, and multinational enterprises.

I regularly speak at conferences including Black Hat, DEF CON, BSides, and OWASP Cairo on topics such as AI red teaming, cloud attack simulation, supply-chain risk, log manipulation, and practical offensive tradecraft. I also design and deliver hands-on training, contribute to security education, and support community initiatives through AI Village, BSides Albuquerque, OWASP Cairo, and CyberDose.

SpeakerBio: Saad Nasir

Saad Nasir is a cybersecurity leader specializing in red teaming, penetration testing, and application security. He currently leads Red Team and Application Security initiatives, overseeing offensive security operations, adversary simulation, and security assessments across enterprise environments.

With more than 10 years of cybersecurity experience, Saad has led offensive security engagements spanning web applications, cloud platforms, internal networks, and Active Directory environments. He is the founder and organizer of Security BSides Albuquerque, helping grow one of New Mexico's largest community-driven cybersecurity conferences.

Saad is pursuing a PhD in National Security and holds a Master's degree in Cybersecurity, along with multiple industry certifications, including OSCP and CISM. He is passionate about sharing practical skills, helping defenders understand the mindset of attackers, and advancing the cybersecurity community through mentoring, conference speaking, and hands-on training.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Burp, But Yours: Hands-On Extension and Bambda Development

Tags: Intermediate | AppSec Village | Creator Workshop

When: Friday, Aug 7, 10:30 - 12:30 PDT

Where: LVCCW Level 1 Hall 2 604 (Appsec Village) Classroom - [Map](#)

Description:

Burp Suite already solves most daily testing problems, but the security landscape constantly evolves. New vulnerabilities, CVEs, and techniques emerge every day, and sometimes the capability you need simply does not exist yet.

In this hands-on workshop, you'll learn how to adapt Burp Suite to your workflow using custom scan checks, Bambdas, extensions, and the BApp Store. You'll create your own Bambdas, test them against Web Security Academy labs, modify a free template extension, and start a project you can continue after the session.

You'll leave with practical tools, a repeatable development approach, and guidance on sharing your work with teammates or the wider community.

SpeakerBio: Hannah L, Burp Suite Extensibility Specialist at PortSwigger

Hannah is an Extensibility Specialist at PortSwigger, where she helps shape how Burp Suite can be adapted to real-world testing workflows. She works hands-on with submissions to the BApp Store, as well as the Bambdas and BChecks community repositories, helping refine extensions and community contributions before they're shared more widely.

She especially enjoys making extensions better and finding creative workarounds to awkward testing problems. She has also written extensions for customers, internal teams, and her own projects, including the original WebSocket Turbo Intruder extension.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Bug Bounty Village - Saturday - 16:00-17:59 PDT

Title: Burp, But Yours: Hands-On Extension and Bambda Development

Tags: Bug Bounty Village | Creator Workshop

When: Saturday, Aug 8, 16:00 - 17:59 PDT

Where: LVCCW Level 2 W206-207 (Bug Bounty Village) - [Map](#)

Description:

Ever found yourself scrolling through thousands of requests looking for the few that matter? Repeating the same checks across every target? Wishing Burp Suite would automate part of your workflow?

This hands-on workshop teaches bug bounty hunters how to build Burp customizations that surface valuable signals and eliminate repetitive work.

SpeakerBio: Hannah L, Burp Suite Extensibility Specialist at PortSwigger

Hannah is an Extensibility Specialist at PortSwigger, where she helps shape how Burp Suite can be adapted to real-world testing workflows. She works hands-on with submissions to the BApp Store, as well as the Bambdas and BChecks community repositories, helping refine extensions and community contributions before they're shared more widely.

She especially enjoys making extensions better and finding creative workarounds to awkward testing problems. She has also written extensions for customers, internal teams, and her own projects, including the original WebSocket Turbo Intruder extension.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Mobile Hacking Community - Friday - 10:00-10:45 PDT

Title: Bypassing KYC Vendors on AI Times

Tags: Mobile Hacking Community | Creator Talk/Panel

When: Friday, Aug 7, 10:00 - 10:45 PDT

Where: LVCCW Level 1 Hall 4 1422 (Mobile Hacking Community) - [Map](#)

Description:

In this talk, the Just Mobile Security team will talk about the KYC implementation, how to bypass them, and some 0 days for vendors.

Speakers: Juan Urbano Stordeur, Juan Martinez Blanco

SpeakerBio: Juan Urbano Stordeur, CEO and Founder at Just Mobile Security

No BIO available

SpeakerBio: Juan Martinez Blanco, Mobile Security Penetration Tester at Just Mobile Security

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: C(2)YA: Inside the Adversary's Inbox

Tags: DEF CON Official Talk | Demo | Exploit

When: Saturday, Aug 8, 12:00 - 12:59 PDT

Where: LVCCW Level 1 Hall 3 903 (Main Track 5) - [Map](#)

Description:

85 findings exploitable from the internet with zero prior access. 28 takedown chains. Crypto failures that let you decrypt all C2 traffic with one recovered key.

Here's how I got there. I'd been using coding agents to find bugs in software. Then I thought: what if I did this from the defender's side, against the tools that threat actors actually use? I pointed LLM-assisted research at five C2 frameworks: Havoc, Mythic, Sliver, Covenant, AdaptixC2. Six months later, 251 design flaws, behavioral weaknesses, and vulnerabilities. Validated every finding in realistic lab environments. Then passively tapped 35 live servers via Shodan and Censys, and found operators running campaigns against victims in education, manufacturing, legal, and biotech across eight countries.

Eight bug classes recur across all five codebases. Findings rated on a defender-weighted scale, because CVSS doesn't tell you which bug finds the server. Havoc, the most-deployed framework in the dataset, was archived on February 21, 2026. No patches coming. Defenders carry the load now.

AI isn't just for protecting systems. Defenders can point it at the attackers' own tools and find real ways to fight back. All findings for maintained projects disclosed through proper channels. Every demo against realistic lab environments I control.

SpeakerBio: Vitaly Simonovich, Cato Networks

Vitaly Simonovich is a Senior Security Researcher at Cato Networks on the CTRL threat research team, following over ten years in cybersecurity across Cato CTRL and Imperva, where he focused on DDoS and botnet research from 2019 to 2023.

He coined HashJack, the first indirect prompt injection weaponizing URL fragments against AI browser assistants, and LAMEHUG, the first LLM-powered malware publicly linked to APT28. He documented the Immersive World jailbreak against Microsoft Copilot and introduced the Zero-Knowledge Threat Actor concept. His research has driven ten coordinated security disclosures across Open WebUI, MongoDB, Jenkins, BIND, Moodle, TYPO3, Perplexity, Microsoft, and others.

His work has been covered by Forbes, The Economist, Business Insider, VentureBeat, The Register, The Hacker News, and CyberScoop.

Conference talks: RSA Conference 2026, Botconf 2022, BSidesTLV 2025 AI Hacking Village, Qubit 2025 Prague, RootedCon 2026.

vitalysim.com

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Cache Key Injection: Smuggling Poison Through the Door

Tags: Bug Bounty Village | Creator Talk/Panel

When: Friday, Aug 7, 15:00 - 15:30 PDT

Where: LVCCW Level 1 Hall 3 1102 (Creator Stage 6) - [Map](#)

Description:

Cache poisoning research has long centred on unkeyed-input injection. The next cache poisoning vulnerability may not come from unkeyed input, but from what is mistakenly included in the cache key itself. This talk explores a lesser-known attack path: cache key injection caused by subtle cache misconfigurations that allow attacker-controlled values to influence keyed cache components. By triggering cache key injection, attackers can perform cache key collisions, leading to cache poisoning and impacts such as CPDoS, cache deception, and stored XSS through poisoned cache keys. I'll show how these collisions can be identified, how they can be exploited to achieve impact, and the mitigations that can be implemented to prevent cache key injection.

Cache poisoning research has long centred on unkeyed-input injection. The next cache poisoning vulnerability may not come from unkeyed input, but from what is mistakenly included in the cache key itself. This talk explores a lesser-known attack path: cache key injection caused by subtle cache misconfigurations that allow attacker-controlled values to influence keyed cache components. By triggering cache key injection, attackers can perform cache key collisions, leading to cache poisoning and impacts such as CPDoS, cache deception, and stored XSS through poisoned cache keys. I'll show how these collisions can be identified, how they can be exploited to achieve impact, and the mitigations that can be implemented to prevent cache key injection.

SpeakerBio: Alex Brumen, YesWeHack

Alex Brumen (aka "Brumens") is a Security Research Enablement Analyst at YesWeHack, where his ethical hacking work focuses primarily on web applications. Outside of work, he is also a bug bounty hunter and developer.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

The Diana Initiative - Friday - 12:40-12:50 PDT

Title: Call Center Tour

Tags: The Diana Initiative | Creator Tour

When: Friday, Aug 7, 12:40 - 12:50 PDT

Where: LVCCW Level 1 South Lobby / Atrium - [Map](#)

Description:

Interested in visiting Call Center but afraid to go by yourself? The Diana Initiative is hosting tours! Follow a volunteer to Call Center and be introduced to the community and activities inside!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Call Center Village - Saturday - 10:00-17:59 PDT

Title: Call Center Village - Open

Tags: Call Center Village | Creator Event/Activity

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 2 W218 (Call Center Village) - [Map](#)

Description:

Security teams have spent years hardening web-apps, email-gateways, and network-perimeters. Meanwhile, the phone line sitting on every receptionist's desk remains almost completely unmonitored. Nobody's deploying a firewall between a caller and the person who picks up. Caller ID authentication has made some progress, but the conversation itself? Wide open.

And now that AI-generated voices can pass for the real thing and automated agents are handling account resets and payment processing, that gap is getting a lot more interesting. Call Center Village is where voice security, conversational AI, and social engineering collide — across both voice and text channels.

Sit down at a workstation and synthesize a copy of your own voice with open-source tools running on a local GPU, or let our staff walk you through the process. Dig into voice pipelines, deepfake audio detection, and the arms race between the two. Wire up a working conversational AI agent — stitching together the real-time audio infrastructure, transcription, language model, and speech synthesis that make these systems speak.

On the text side, go after chatbot agents tasked with handling simulated customer interactions. Find the cracks in their system prompts, hijack conversation logic, and convince them to do things their developers never intended. Once you're ready, muster all your skills to take on our Escalation Desk CTF, the official Call Center Village contest at DEF CON 34.

We've also got a collection of vintage telephones, prank extensions, chatty AI-agents, and a British-style telephone booth worth stopping by for.

No prior experience required. If you know how to make a phone call or type a message, you're already qualified. Equipment is provided, including laptops and ANC headsets - but you're more than welcome to bring your own devices.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Call Center Village - Friday - 10:00-17:59 PDT

Title: Call Center Village - Open

Tags: Call Center Village | Creator Event/Activity

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 2 W218 (Call Center Village) - [Map](#)

Description:

Security teams have spent years hardening web-apps, email-gateways, and network-perimeters. Meanwhile, the phone line sitting on every receptionist's desk remains almost completely unmonitored. Nobody's deploying a firewall between a caller and the person who picks up. Caller ID authentication has made some progress, but the conversation itself? Wide open.

And now that AI-generated voices can pass for the real thing and automated agents are handling account resets and payment processing, that gap is getting a lot more interesting. Call Center Village is where voice security, conversational AI, and social engineering collide — across both voice and text channels.

Sit down at a workstation and synthesize a copy of your own voice with open-source tools running on a local GPU, or let our staff walk you through the process. Dig into voice pipelines, deepfake audio detection, and the arms race between the two. Wire up a working conversational AI agent — stitching together the real-time audio infrastructure, transcription, language model, and speech synthesis that make these systems speak.

On the text side, go after chatbot agents tasked with handling simulated customer interactions. Find the cracks in their system prompts, hijack conversation logic, and convince them to do things their developers never intended. Once you're ready, muster all your skills to take on our Escalation Desk CTF, the official Call Center Village contest at DEF CON 34.

We've also got a collection of vintage telephones, prank extensions, chatty AI-agents, and a British-style telephone booth worth stopping by for.

No prior experience required. If you know how to make a phone call or type a message, you're already qualified. Equipment is provided, including laptops and ANC headsets - but you're more than welcome to bring your own devices.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Call Center Village - Sunday - 10:00-13:59 PDT

Title: Call Center Village - Open

Tags: Call Center Village | Creator Event/Activity

When: Sunday, Aug 9, 10:00 - 13:59 PDT

Where: LVCCW Level 2 W218 (Call Center Village) - [Map](#)

Description:

Security teams have spent years hardening web-apps, email-gateways, and network-perimeters. Meanwhile, the phone line sitting on every receptionist's desk remains almost completely unmonitored. Nobody's deploying a firewall between a caller and the person who picks up. Caller ID authentication has made some progress, but the conversation itself? Wide open.

And now that AI-generated voices can pass for the real thing and automated agents are handling account resets and payment processing, that gap is getting a lot more interesting. Call Center Village is where voice security, conversational AI, and social engineering collide — across both voice and text channels.

Sit down at a workstation and synthesize a copy of your own voice with open-source tools running on a local GPU, or let our staff walk you through the process. Dig into voice pipelines, deepfake audio detection, and the arms race between the two. Wire up a working conversational AI agent — stitching together the real-time audio infrastructure, transcription, language model, and speech synthesis that make these systems speak.

On the text side, go after chatbot agents tasked with handling simulated customer interactions. Find the cracks in their system prompts, hijack conversation logic, and convince them to do things their developers never intended. Once you're ready, muster all your skills to take on our Escalation Desk CTF, the official Call Center Village contest at DEF CON 34.

We've also got a collection of vintage telephones, prank extensions, chatty AI-agents, and a British-style telephone booth worth stopping by for.

No prior experience required. If you know how to make a phone call or type a message, you're already qualified. Equipment is provided, including laptops and ANC headsets - but you're more than welcome to bring your own devices.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Can AI do novel security research? Meet the HTTP Terminator

Tags: DEF CON Official Talk | Tool | Exploit

When: Friday, Aug 7, 12:00 - 12:59 PDT

Where: LVCCW Level 1 Hall 3 906 (Main Track 3) - [Map](#)

Description:

We all know AI can find bugs. After a decade of research, I asked a harder question: can an autonomous system invent new attack techniques, and use them to hack live websites at scale? Building this sounded like a bad idea, so I did it.

It worked - I'll share an arsenal of new HTTP desync triggers, gadgets, and exploits that compromised banks, security solutions, and government infrastructure. Then I'll trace each discovery chain back through the HTTP Terminator, showing how to turn your personal expertise into an autonomous weapon - and the dark arts required to make it lethal.

I'll also share discoveries from beyond the autonomy horizon - some only reachable with a tight human/AI research loop, and others beyond AI's reach entirely. These include a powerful undisclosed recon technique, and anomalies that hint at new attack classes offering alternative paths to critical impact. I'll analyse the discovery process, sharing detailed experiments that probe the boundaries of what AI can and can't discover.

You'll leave with new exploits from desync triggers to undisclosed attack classes, and a blueprint for turning your instincts into an autonomous research cascade. And yes, I'll open-source the HTTP Terminator.

<https://portswigger.net/research/http1-must-die>

<https://i.blackhat.com/BH-USA-25/Presentations/US-25-Dolan-Gavitt-AI-Agents-for-Offsec-with-Zero-False-Positives-Thursday.pdf>

<https://portswigger.net/research/listen-to-the-whispers-web-timing-attacks-that-actually-work>

<https://www.intruder.io/research/practical-http-header-smuggling>

SpeakerBio: James "albinowax" Kettle, PortSwigger

James 'albinowax' Kettle is the Director of Research at PortSwigger, the makers of Burp Suite. He's best known for pioneering novel web attack techniques, and publishing them at major conferences like Black Hat USA, at which he's presented for nine consecutive years.

He also loves exploring and advising on innovative tool concepts for security professionals, many of which have since become industry standard. Examples include introducing OAST via Burp Collaborator, bulk parameter discovery via Param Miner, billion-request attacks with Turbo Intruder, and human-style scanning with Backslash Powered Scanner.

His best-known research is HTTP Desync Attacks, which popularised HTTP Request Smuggling. Other popular attack techniques that can be traced back to his research include web cache poisoning, the single-packet attack, server-side template injection, and password reset poisoning. He's also the designer behind many of the topics and labs that make up the Web Security Academy, and serves on the Black Hat Europe review board.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Payment Village - Sunday - 12:00-12:15 PDT

Title: CAPTURE THE COIN - Announcement of the CTF Winners

Tags: Payment Village | \$\$\$\$\$_\$\$\$\$\$ | Creator Talk/Panel

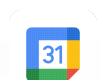
When: Sunday, Aug 9, 12:00 - 12:15 PDT

Where: LVCCW Level 2 W204-205 (Payment Village) - [Map](#)

Description:

Join us as we announce the winners of the Contest!

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

DEF CON Training - Tuesday - 08:30-17:30 PDT

Title: Car Hacking Masterclass - Attacking & Defending Automotive Systems and Infrastructure

Tags: DEF CON Training (Paid) (2-day) | DEF CON Training

When: Tuesday, Aug 11, 08:30 - 17:30 PDT

Where: LVCCW Level 2 W222 (Workshops) - [Map](#)

Description:

SpeakerBio: Kamel Ghali

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

DEF CON Training - Monday - 08:30-17:30 PDT

Title: Car Hacking Masterclass - Attacking & Defending Automotive Systems and Infrastructure

Tags: DEF CON Training (Paid) (2-day) | DEF CON Training

When: Monday, Aug 10, 08:30 - 17:30 PDT

Where: LVCCW Level 2 W222 (Workshops) - [Map](#)

Description:

SpeakerBio: Kamel Ghali

No BIO available



[Return to Index](#) - Add to Google

- ics [Calendar](#) file

Contests - Saturday - 10:00-16:59 PDT

Title: Car Hacking Village CTF

Tags: Car Hacking Village | Car Hacking Village Capture the Flag (CTF) | Contest

When: Saturday, Aug 8, 10:00 - 16:59 PDT

Where: LVCCW Level 1 Hall 2 701 (Car Hacking Village) - [Map](#)

Description:

Participate in CHV's CTF to learn and play with automotive technology. This year's contest features problems on smart chargers, automotive ECU harnesses, our own badge, and more! Don't worry about bringing your own automotive specific gear, we've got you covered. Stop by the village to register, get started, and get hacking.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Contests - Friday - 10:00-16:59 PDT

Title: Car Hacking Village CTF

Tags: Car Hacking Village | Car Hacking Village Capture the Flag (CTF) | Contest

When: Friday, Aug 7, 10:00 - 16:59 PDT

Where: LVCCW Level 1 Hall 2 701 (Car Hacking Village) - [Map](#)

Description:

Participate in CHV's CTF to learn and play with automotive technology. This year's contest features problems on smart chargers, automotive ECU harnesses, our own badge, and more! Don't worry about bringing your own automotive specific gear, we've got you covered. Stop by the village to register, get started, and get hacking.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Contests - Sunday - 10:00-11:59 PDT

Title: Car Hacking Village CTF

Tags: Car Hacking Village | Car Hacking Village Capture the Flag (CTF) | Contest

When: Sunday, Aug 9, 10:00 - 11:59 PDT

Where: LVCCW Level 1 Hall 2 701 (Car Hacking Village) - [Map](#)

Description:

Participate in CHV's CTF to learn and play with automotive technology. This year's contest features problems on smart chargers, automotive ECU harnesses, our own badge, and more! Don't worry about bringing your own automotive specific gear, we've got you covered. Stop by the village to register, get started, and get hacking.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Car Hacking Village - Sunday - 10:00-13:59 PDT

Title: Car Hacking Village Open

Tags: Car Hacking Village | Creator Event/Activity

When: Sunday, Aug 9, 10:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 2 701 (Car Hacking Village) - [Map](#)

Description:

Welcome to the Car Hacking Village - a place where you can learn all about the cool technology that powers modern connected transportation. The CHV at DEF CON 34 will feature a whole race track of activities including Creator Stage presentations, a competitive CTF (with awesome prizes!), an amazing badge for sale that doubles as a fully functional car hacking tool, a scavenger hunt, and more!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Car Hacking Village - Saturday - 10:00-17:59 PDT

Title: Car Hacking Village Open

Tags: Car Hacking Village | Creator Event/Activity

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 2 701 (Car Hacking Village) - [Map](#)

Description:

Welcome to the Car Hacking Village - a place where you can learn all about the cool technology that powers modern connected transportation. The CHV at DEF CON 34 will feature a whole race track of activities including Creator Stage presentations, a competitive CTF (with awesome prizes!), an amazing badge for sale that doubles as a fully functional car hacking tool, a scavenger hunt, and more!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Car Hacking Village - Friday - 10:00-17:59 PDT

Title: Car Hacking Village Open

Tags: Car Hacking Village | Creator Event/Activity

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 2 701 (Car Hacking Village) - [Map](#)

Description:

Welcome to the Car Hacking Village - a place where you can learn all about the cool technology that powers modern connected transportation. The CHV at DEF CON 34 will feature a whole race track of activities including Creator Stage presentations, a competitive CTF (with awesome prizes!), an amazing badge for sale that doubles as a fully functional car hacking tool, a scavenger hunt, and more!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

DEF CON Talks - Saturday - 10:00-11:59 PDT

Title: Car Hacking Village Scavenger Hunt Contest

Tags: DEF CON Official Talk | Car Hacking Village

When: Saturday, Aug 8, 10:00 - 11:59 PDT

Where: LVCCW Level 1 Hall 2 701 (Car Hacking Village) - [Map](#)

Description:

Go out and find some goofy stuff!!

The DEF CON 34 CHV Scavenger Hunt rules and treasure list can be found at the attached link.

Start Time: Friday, August 7 10:00

End Time: Sunday, August 9: 12:00

One Car Hacking Village 2026 Badge will be awarded to the first player to complete the Scavenger Hunt!

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

DEF CON Talks - Friday - 10:00-11:59 PDT

Title: Car Hacking Village Scavenger Hunt Contest

Tags: DEF CON Official Talk | Car Hacking Village

When: Friday, Aug 7, 10:00 - 11:59 PDT

Where: LVCCW Level 1 Hall 2 701 (Car Hacking Village) - [Map](#)

Description:

Go out and find some goofy stuff!!

The DEF CON 34 CHV Scavenger Hunt rules and treasure list can be found at the attached link.

Start Time: Friday, August 7 10:00

End Time: Sunday, August 9: 12:00

One Car Hacking Village 2026 Badge will be awarded to the first player to complete the Scavenger Hunt!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

The Diana Initiative - Friday - 12:30-12:40 PDT

Title: Car Hacking Village Tour

Tags: The Diana Initiative | Creator Tour

When: Friday, Aug 7, 12:30 - 12:40 PDT

Where: LVCCW Level 1 South Lobby / Atrium - [Map](#)

Description:

Interested in visiting Car Hacking Village but afraid to go by yourself? The Diana Initiative is hosting tours! Follow a volunteer to Car Hacking Village and be introduced to the community and activities inside!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Cards Against Vulnerabilities

Tags: AppSec Village | Creator Event/Activity | All Audiences

When: Friday, Aug 7, 13:00 - 14:59 PDT

Where: LVCCW Level 1 Hall 2 604 (Appsec Village) POD 1 - [Map](#)

Description:

Join us for "Cards Against Security: Trust Me, It's Secure," a hilarious card game inspired by Cards Against Humanity! Test your wit as you create the funniest responses to prompts related to software development and security. Gather your friends at the AppSec Village and dive into a world of Chainguard humor. Compete to be the first to five points and win bragging rights (and prizes)! Don't miss out on this fun-filled experience that combines laughter with learning—perfect for security enthusiasts and developers alike!

SpeakerBio: Patrick Smyth

Dr. Patrick Smyth is Principal Developer Relations Engineer at Chainguard, where he shows developers how to deploy AI and other applications with 0 CVEs using Chainguard Images. Patrick has a PhD in the digital humanities and in a previous life led technical bootcamps for researchers at Columbia University. In his free time you can find Patrick swimming in a frozen lake or hanging out with his six-month-old baby.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Cards Against Vulnerabilities

Tags: AppSec Village | Creator Event/Activity | All Audiences

When: Friday, Aug 7, 11:00 - 12:59 PDT

Where: LVCCW Level 1 Hall 2 604 (Appsec Village) POD 1 - [Map](#)

Description:

Join us for "Cards Against Security: Trust Me, It's Secure," a hilarious card game inspired by Cards Against Humanity! Test your wit as you create the funniest responses to prompts related to software development and security. Gather your friends at the AppSec Village and dive into a world of Chainguard humor. Compete to be the first to five points and win bragging rights (and prizes)! Don't miss out on this fun-filled experience that combines laughter with learning—perfect for security enthusiasts and developers alike!

SpeakerBio: Patrick Smyth

Dr. Patrick Smyth is Principal Developer Relations Engineer at Chainguard, where he shows developers how to deploy AI and other applications with 0 CVEs using Chainguard Images. Patrick has a PhD in the digital humanities and in a previous life led technical bootcamps for researchers at Columbia University. In his free time you can find Patrick swimming in a frozen lake or hanging out with his six-month-old baby.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Cards Against Vulnerabilities

Tags: AppSec Village | Creator Event/Activity || All Audiences

When: Friday, Aug 7, 15:00 - 16:59 PDT

Where: LVCCW Level 1 Hall 2 604 (Appsec Village) POD 1 - [Map](#)

Description:

Join us for "Cards Against Security: Trust Me, It's Secure," a hilarious card game inspired by Cards Against Humanity! Test your wit as you create the funniest responses to prompts related to software development and security. Gather your friends at the AppSec Village and dive into a world of Chainguard humor. Compete to be the first to five points and win bragging rights (and prizes)! Don't miss out on this fun-filled experience that combines laughter with learning—perfect for security enthusiasts and developers alike!

SpeakerBio: Patrick Smyth

Dr. Patrick Smyth is Principal Developer Relations Engineer at Chainguard, where he shows developers how to deploy AI and other applications with 0 CVEs using Chainguard Images. Patrick has a PhD in the digital humanities and in a previous life led technical bootcamps for researchers at Columbia University. In his free time you can find Patrick swimming in a frozen lake or hanging out with his six-month-old baby.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Cards Against Vulnerabilities

Tags: AppSec Village | Creator Event/Activity | All Audiences

When: Saturday, Aug 8, 11:00 - 12:59 PDT

Where: LVCCW Level 1 Hall 2 604 (Appsec Village) POD 3 - [Map](#)

Description:

Join us for "Cards Against Security: Trust Me, It's Secure," a hilarious card game inspired by Cards Against Humanity! Test your wit as you create the funniest responses to prompts related to software development and security. Gather your friends at the AppSec Village and dive into a world of Chainguard humor. Compete to be the first to five points and win bragging rights (and prizes)! Don't miss out on this fun-filled experience that combines laughter with learning—perfect for security enthusiasts and developers alike!

SpeakerBio: Patrick Smyth

Dr. Patrick Smyth is Principal Developer Relations Engineer at Chainguard, where he shows developers how to deploy AI and other applications with 0 CVEs using Chainguard Images. Patrick has a PhD in the digital humanities and in a previous life led technical bootcamps for researchers at Columbia University. In his free time you can find Patrick swimming in a frozen lake or hanging out with his six-month-old baby.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

IoT Village - Friday - 10:00-17:59 PDT

Title: Cat-astrophic Hacking: Breaking Into Smart Litter Boxes

Tags: IoT Village | Creator Event/Activity

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 215 (IoT Village) - [Map](#)

Description:

What happens when your cat's litter box joins the Internet of Things? Join Suzu Labs as we dissect, analyze, and hack smart litter robots to uncover security risks.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

IoT Village - Sunday - 10:00-13:59 PDT

Title: Cat-astrophic Hacking: Breaking Into Smart Litter Boxes

Tags: IoT Village | Creator Event/Activity

When: Sunday, Aug 9, 10:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 1 215 (IoT Village) - [Map](#)

Description:

What happens when your cat's litter box joins the Internet of Things? Join Suzu Labs as we dissect, analyze, and hack smart litter robots to uncover security risks.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

IoT Village - Saturday - 10:00-17:59 PDT

Title: Cat-apstrophic Hacking: Breaking Into Smart Litter Boxes

Tags: IoT Village | Creator Event/Activity

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 215 (IoT Village) - [Map](#)

Description:

What happens when your cat's litter box joins the Internet of Things? Join Suzu Labs as we dissect, analyze, and hack smart litter robots to uncover security risks.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Catching Cheaters in Super Smash Bros Melee

Tags: Game Hacking Village | Creator Talk/Panel

When: Saturday, Aug 8, 14:00 - 14:59 PDT

Where: LVCCW Level 1 Hall 1 211 (Game Hacking Village) - [Map](#)

Description:

Super Smash Bros Melee for the Nintendo GameCube is one of the oldest active fighting game communities, with a storied 25 year history.

Would you believe that people try to cheat at it?!

I am the maintainer of the SLP Enforcer tool, and help with cheating investigations for the community. I'm going to share some stories of people trying to cheat and getting caught! Along the way I'll describe all the ways one could try to cheat at Melee, and how our detection tools work.

SpeakerBio: AltF4

Dan "AltF4" Petro is a Principal Security Engineer at Bishop Fox R&D. As a longtime pentester at Bishop Fox, Dan's presented public research on everything from hacking into smart safes, compromising the power grid, breaking into secure facilities, and cheating at online video games. There was even that time he found a vulnerability in (nearly) every IoT device. But Dan's favorite research project is always whichever is next.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Catching Cheaters in Super Smash Bros Melee

Tags: Game Hacking Village | Creator Talk/Panel

When: Saturday, Aug 8, 11:30 - 11:59 PDT

Where: LVCCW Level 1 Hall 3 801 (Creator Stage 2) - [Map](#)

Description:

Super Smash Bros Melee for the Nintendo GameCube is one of the oldest active fighting game communities, with a storied 25 year history.

Would you believe that people try to cheat at it?!

I am the maintainer of the SLP Enforcer tool, and help with cheating investigations for the community. I'm going to share some stories of people trying to cheat and getting caught! Along the way I'll describe all the ways one could try to cheat at Melee, and how our detection tools work.

SpeakerBio: AltF4

Dan "AltF4" Petro is a Principal Security Engineer at Bishop Fox R&D. As a longtime pentester at Bishop Fox, Dan's presented public research on everything from hacking into smart safes, compromising the power grid, breaking into secure facilities, and cheating at online video games. There was even that time he found a vulnerability in (nearly) every IoT device. But Dan's favorite research project is always whichever is next.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Certified Re-Pwned: escalating all the way up

Tags: DEF CON Official Talk | Demo | Tool

When: Friday, Aug 7, 16:00 - 16:59 PDT

Where: LVCCW Level 1 Hall 3 906 (Main Track 3) - [Map](#)

Description:

Four years after KB5014754 and one year after CVE-2024-49019, every hardening guide says Active Directory Certificate Services is a closed book. This talk reopens it.

We present five new primitives — proposed as ESC18 through ESC22, extending the public ESC1–ESC17 numbering — each validated end-to-end on a fully-patched Windows Server 2025 Enterprise CA with every Microsoft-recommended mitigation applied. Every primitive starts from a Domain Users account with no ACL, GPO, or template edges, and ends at `krbtgt` extraction.

Each primitive targets a different component of the post-2022 defence: the CA's CSR processor, the CA's Security-Extension writer, the KDC's PKINIT binder, the CA's Enroll-On-Behalf-Of path, and the registry-level enforcement layer everyone thinks is already hardened. Together they argue that Microsoft's 2022 and 2024 fixes patched specific instances of the underlying bug classes, not the classes themselves — and that at least one control has an undocumented fallback path its own documentation does not mention.

A Certipy research fork will be released at the time of the talk to check and exploit the new techniques.

<https://posts.specterops.io/certified-pre-owned-d95910965cd2>

https://specterops.io/wp-content/uploads/sites/3/2022/06/Certified_Pre-Owned.pdf

<https://support.microsoft.com/en-us/topic/kb5014754-certificate-based-authentication-changes-on-windows-domain-controllers-ad>

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49019>

<https://posts.specterops.io/adcs-esc13-abuse-technique-fda4272fbd53> <https://github.com/ly4k/Certipy>

Speakers: Daniel Monzon, Eric Labrador

SpeakerBio: Daniel Monzon

Daniel Monzón (stark0de) — Offensive Security Engineer at Halborn with 6+ years of offensive security experience across web pentesting, code review, Active Directory (on-premise and hybrid), Android/iOS mobile audits, thick-client assessments and red teaming. Holds certifications such as: OSCP, CRTP, OSWP, CREST CPSA, eMAPT, PACSP, and CARTP. Has been credited with multiple CVEs in open-source and commercial products, and currently focuses on Web3 and financial-sector security. Prior speaker at hack0n, RootedCON Málaga, DragonJARCON, and SecAdmin.

SpeakerBio: Eric Labrador

Eric Labrador is an offensive security researcher at Accenture with over 6 years of experience breaking into networks, applications, and buildings for a living. His day-to-day work covers Red and Purple Team exercises, web and API audits, Android and iOS mobile application assessments, internal and external penetration testing, physical intrusions into corporate buildings, and large-scale phishing campaigns. He holds the OSCP, CRTE, CRT0, BSCP, and eWPTXv2 certifications, and is the author of ImagePanick, an open-source exploit chain that achieves arbitrary file write and remote code execution by combining weak default policies in ImageMagick with SAFER bypasses in Ghostscript, all triggered from a malicious SVG. Over the years he has delivered end-to-end attack paths that chain phishing, external footholds, lateral movement, and physical entry into full compromise across multiple industries, helping clients understand what a motivated attacker can actually do with the people, processes, and technology already in place.



Title: Chaining Credentials Through the AI Infrastructure Nobody Secured

Tags: Red Team Village | Misc

When: Saturday, Aug 8, 14:00 - 14:59 PDT

Where: LVCCW Level 1 Hall 1 309 (Red Team Village) Workshop Stage 2 - [Map](#)

Description:

AI/ML services are proliferating across enterprise networks without security review. Developers deploy Ollama instances locally, data science teams stand up Jupyter notebooks and MLflow registries without authentication, platform engineers run Ray clusters and LiteLLM API gateways on default configurations, and MCP tool servers expose file system access and code execution to the network. These services rarely appear in traditional vulnerability scans and are seldom included in asset inventories.

To measure the scope of this problem, I built a 5-VM benchmark lab simulating four independent teams deploying 19 AI/ML endpoints with 122 planted findings. The lab includes a manifest-driven scoring harness that enables objective detection measurement across three validation modes: standard (substring matching), strict (host attribution and source module accuracy), and contract (workflow metadata and evidence chain verification).

The tool is `aipostex`, an open-source single-binary Go framework designed for the full AI infrastructure attack lifecycle. It performs network discovery across 20+ AI service families, executes 123 vulnerability templates, and provides 17 dedicated exploit modules covering Ollama, Jupyter, MCP servers, LiteLLM gateways, MLflow, Ray, vector databases, and inference endpoints. MCP coverage includes schema poisoning, environment variable extraction, and CVE-specific checks for DNS rebinding and remote code execution through tool servers. A separate model-scan capability identifies deserialization risk in pickle, PyTorch, TensorFlow, and ONNX model files.

The live demonstration walks through a credential chain attack against the benchmark lab. The attack begins with Ray cluster enumeration to harvest API keys from job environment variables, pivots into MLflow where experiment run parameters and tags contain embedded secrets and cloud credentials, then chains those tokens to authenticate against a HuggingFace TGI inference endpoint. Each hop crosses a different team's infrastructure, discovered and linked by the tool's credential chain-loading engine.

The session also covers the safety and operational controls that make this suitable for production engagements: explicit `--force-exploit` gating on mutating actions, `--mode full` requirement for exploit templates, proof-strength classification on every finding (reachable, read-confirmed, execution-confirmed), and OPSEC features including User-Agent rotation, TLS fingerprint randomization, and timing jitter.

Open-source release coinciding with presentation.

Does your workshop come with a tactic?

Yes. The tactic is "Hands-On: Credential Chain Exploitation Across Shadow AI Infrastructure."

Each group of about five attendees gets their own isolated cloud-hosted lab instance, a full 5-VM environment spun up on AWS and accessible only through a VPN tunnel. You SSH into your group's attack box and work through a guided attack chain against the lab's 19 AI/ML endpoints.

First, you scan the /24 and discover what's running across four target hosts. The tool fingerprints each endpoint and gives you structured next steps, so even if you've never touched MLflow or Ray before, you know what to run next.

Then you follow the credential chain. Enumerate a Ray cluster and pull API keys from job environment variables. Take those into MLflow and extract secrets from experiment run parameters and tags. Chain the tokens forward to authenticate against a

HuggingFace TGI inference endpoint. Three hops, three teams' infrastructure, all connected.

At the end, you run the scoring harness against your results and see how you did. Detection rate, missed findings, proof-strength breakdown, all compared against the 122-finding answer key.

Groups that finish the guided chain early can explore additional attack surfaces across the lab's remaining endpoints, including MCP schema poisoning, Jupyter cell secret mining, and vector database injection. The scoring harness covers all 122 findings, not just the guided path, so there is plenty of room to improve your score.

Each wave runs about 50 minutes with a 10-minute reset between waves. I'll run two waves. All you need is a laptop with an SSH client and a WireGuard client. No prior AI/ML experience required. Everything you use during the tactic, the tool binary, lab docs, and scoring harness, is yours to take home and run on your own infrastructure.

<https://professor-moody.github.io/aipostex/>

<https://professor-moody.github.io/aipostex-lab/>

SpeakerBio: Nathan Keys

Nathan is a security researcher focused on ML supply-chain security. Their research spans information hiding in model artifacts, data poisoning of retrieval pipelines, and post-exploitation of AI infrastructure. Nathan is currently a principal penetration tester in the financial sector. This is their first DEF CON talk. Outside of his passion for research, Nathan loves to touch grass, read all manner of scientific study or journal, and listen to old school southern rap (think UGK). Nathan has changed careers more than once, from winemaking to restaurants to professional hacking now for the last seven years, and he loves a good story and a good conversation.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Chaining Logical Bugs for Reliable Windows LPE

Tags: DEF CON Official Talk | Demo | Exploit

When: Sunday, Aug 9, 13:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 3 903 (Main Track 5) - [Map](#)

Description:

Modern Windows exploit mitigations have made memory corruption significantly harder, but reliable privilege escalation still emerges from a quieter class of bugs: logical flaws in privileged components. This talk shows how low impact Windows bugs become practical SYSTEM exploits when treated as reusable primitives over privileged resources.

We will walk through two distinct LPE chains to illustrate this concept. First, we demonstrate a novel LPE approach achieved by chaining service-level process termination with arbitrary file deletion. Second, we explore another powerful LPE path that leverages kernel- and task-driven registry creation and deletion primitives, ultimately turning attacker-controlled registry state into code execution via Performance DLL hijacking.

- ZDI-24-1098: <https://www.zerodayinitiative.com/advisories/ZDI-24-1098/>
- ZDI-24-451 / CVE-2024-30033: <https://www.zerodayinitiative.com/advisories/ZDI-24-451/>
- CVE-2025-60705: Windows Client-Side Caching Elevation of Privilege Vulnerability
- CVE-2025-59512: Windows Arbitrary Registry Deletion Elevation of Privilege Vulnerability
- Public Microsoft / MSRC security update references for patched issues
- itm4n, "Windows RpcEptMapper Service Insecure Registry Permissions EoP": <https://itm4n.github.io/windows-registry-rpceptmapper-eop/>
- itm4n, "An Unconventional Exploit for the RpcEptMapper Registry Key Vulnerability": <https://itm4n.github.io/windows-registry-rpceptmapper-exploit/>

Speakers:Bocheng "Crispr" Xiang,HeeChan "heegong123" Kim

SpeakerBio: Bocheng "Crispr" Xiang, Fudan Univeristy

Bocheng Xiang (@crispr_x) is a PhD candidate at Fudan University. He is listed on the MSRC MVR 2024/2025 and ranked Top #20 on the MSRC 2024 Q3 Windows Leaderboard. He has published papers at USENIX Security 2025, and his works have been accepted by PoC2025, re//verse2026 and BlackHat USA/Europe.

SpeakerBio: HeeChan "heegong123" Kim, TeamH4C

HeeChan Kim is a security researcher and a student at Soongsil University, specializing in Windows OS internals and Local Privilege Escalation (LPE). As a winner of the DEF CON 33 CTF with team MMM and a member of TeamH4C, he actively hunts for zero-days and persistent logical flaws within complex OS architectures. He has previously presented his Windows LPE research at POC and RE//verse.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Chaining Microsoft Binaries to get Privileged Primitives in the Windows kernel

Tags: DEF CON Official Talk | Demo | Exploit

When: Sunday, Aug 9, 12:30 - 13:30 PDT

Where: LVCCW Level 1 Hall 3 904 (Main Track 4) - [Map](#)

Description:

System Guard Runtime Monitor was meant to be an OS integrity anchor on Windows. A kernel driver, gated behind Protected Process Light (PPL), and a runtime attestation engine running in a secure enclave. In this talk, we revisit a classic code injection technique and adapt it into what we call "Bring Your Own Vulnerable WerFaultSecure". Instead of loading a third-party vulnerable driver, we bring our own vulnerable copy of a PPL-enabled Microsoft binary and its dependencies to get code execution as a protected process. From there, we pivot into the Microsoft System Guard kernel driver, a component that was built to support the integrity attestation of kernel objects, specifically processes, but which can be abused to tamper with those exact objects instead. We will close by sharing Indicators of Compromise (IOCs), along with prevention and detection ideas for defenders, and by discussing the innovation this exploit chain brings to the offensive security landscape.

<https://infocon.org/mirrors/vx%20underground%20-%202025%20June/Papers/Windows/Internals%20and%20Analysis/2022-08-0>

<https://www.microsoft.com/en-us/security/blog/2018/04/19/introducing-windows-defender-system-guard-runtime-attestation/>

<https://googleprojectzero.blogspot.com/2018/10/injecting-code-into-windows-protected.html>

<https://googleprojectzero.blogspot.com/2018/11/injecting-code-into-windows-protected.html>

<https://x.com/GabrielLandau/status/1683854578767343619> <https://blog.scrt.ch/2023/03/17/bypassing-ppl-in-userland-again/>

<https://iamelli0t.github.io/2021/04/10/RPC-Bypass-CFG.html>

<https://github.com/Slowerzs/PPLSystem> https://github.com/mdsecactivebreach/com_inject/

<https://helgeklein.com/blog/anatomy-of-werfault-exe-application-crash-error-reporting/>

SpeakerBio: Angelo Frasca Caccia, SentinelOne

Angelo is a security researcher specialized in Windows Internals. He currently works at SentinelOne, where he conducts research on advanced exploits and tampering techniques targeting the Windows ecosystem. Angelo's background also includes web application penetration testing and red teaming, particularly assume-breach adversary simulations.

Angelo is eCXD, eCPPT, eJPT and OSCP certified. He enjoys reverse engineering and programming, mostly in C/C++. His GitHub profile (<https://github.com/lem0nSec>) features his main contributions to the cybersecurity community.

Angelo has a master's degree in International Security Studies from University of Leicester, where he graduated in 2021 with the 'Best Campus-Based Masters Dissertation Prize' and the 'Best Campus-Based Masters Student Performance Prize'.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Game Hacking Village - Friday - 10:00-15:59 PDT

Title: Chill Zone: Casual Games & TASBot Smash Demo

Tags: Game Hacking Village | Creator Event/Activity

When: Friday, Aug 7, 10:00 - 15:59 PDT

Where: LVCCW Level 1 Hall 1 211 (Game Hacking Village) - [Map](#)

Description:

DEF CON got you overwhelmed? Come relax and play Project Plus, a modded version of Super Smash Bros Brawl. Or compete against a frame perfect Smash Bot!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Game Hacking Village - Saturday - 10:00-15:59 PDT

Title: Chill Zone: Casual Games & TASBot Smash Demo

Tags: Game Hacking Village | Creator Event/Activity

When: Saturday, Aug 8, 10:00 - 15:59 PDT

Where: LVCCW Level 1 Hall 1 211 (Game Hacking Village) - [Map](#)

Description:

DEF CON got you overwhelmed? Come relax and play Project Plus, a modded version of Super Smash Bros Brawl. Or compete against a frame perfect Smash Bot!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Game Hacking Village - Saturday - 16:00-16:59 PDT

Title: Chill Zone: Smash (Project Plus) Tournament with Prizes

Tags: Game Hacking Village | Creator Event/Activity

When: Saturday, Aug 8, 16:00 - 16:59 PDT

Where: LVCCW Level 1 Hall 1 211 (Game Hacking Village) - [Map](#)

Description:

Compete against other attendees in a modded version of Super Smash Bros Brawl! This is a low stakes tourney that is beginner friendly and open to all.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Game Hacking Village - Friday - 16:00-16:59 PDT

Title: Chill Zone: Smash (Project Plus) Tournament with Prizes

Tags: Game Hacking Village | Creator Event/Activity

When: Friday, Aug 7, 16:00 - 16:59 PDT

Where: LVCCW Level 1 Hall 1 211 (Game Hacking Village) - [Map](#)

Description:

Compete against other attendees in a modded version of Super Smash Bros Brawl! This is a low stakes tourney that is beginner friendly and open to all.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Blacks In Cyber Village - Saturday - 15:00-15:55 PDT

Title: ChronoRoot: Time-Traveling Through Kernel Trust Boundaries

Tags: Blacks In Cyber Village | Creator Talk/Panel

When: Saturday, Aug 8, 15:00 - 15:55 PDT

Where: LVCCW Level 3 W322-W324 (BIC Village) - [Map](#)

Description:

Join B.I.C. Village for ChronoRoot: Time-Traveling Through Kernel Trust Boundaries, a welcoming session focused on kernel trust boundaries, system internals, and how attackers challenge low-level security assumptions. Come ready to learn, ask questions, and connect with the community.

Speakers: Ahmeen Muhammad, Sydney Johns

SpeakerBio: Ahmeen Muhammad, Cybersecurity Professional / Community Speaker

Ahmeen C. Muhammad is a Senior Penetration Testing Consultant and Army cyber veteran with experience conducting offensive security operations across enterprise and government environments. His interests include red teaming, reverse engineering, Malware Development, endpoint security evasion, and AI security testing. When he's not on an engagement, Ahmeen spends his time researching emerging attack techniques, developing offensive tooling, and sharing knowledge with the cybersecurity community. He is passionate about helping organizations better understand their security posture through realistic adversary emulation and hands-on offensive security research.

SpeakerBio: Sydney Johns, AI/ML Engineer, Virginia Tech Researcher

Sydney Johns is an Artificial Intelligence Researcher at GitHub and a Ph.D. student in Computer Science at Virginia Tech. Her research interests include artificial intelligence, machine learning, reverse engineering, and ethical hacking. She holds a Bachelor's degree in Electrical Engineering and a Master's degree in Cybersecurity, along with CompTIA Security+ and EC-Council Certified Ethical Hacker certifications. Sydney is passionate about STEM outreach, mentorship, and creating pathways for more people to enter technology and cybersecurity. In her spare time, she enjoys playing Overcooked and Animal Crossing, painting, and shopping.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Cirro: Extending Your Azure Graph Beyond Identities

Tags: Demo | Cloud Village | Creator Event/Activity | Tool | Attack | Tools

When: Friday, Aug 7, 16:00 - 17:59 PDT

Where: LVCCW Level 3 W311 (Cloud Village Labs) A - [Map](#)

Description:

Most Azure graph analysis tooling focuses primarily on identity relationships: users, groups, service principals, and role assignments. While valuable, modern Azure environments contain far more exploitable context hidden within infrastructure, platform services, application configurations, network relationships, managed identities, and data-plane resources.

Cirro (the spiritual successor to Stormspotter) is an attack graphing tool built to model Azure environments by combining Microsoft Graph identity data with Azure Resource Manager (ARM) infrastructure data. Instead of limiting analysis to Entra ID objects and role assignments, Cirro maps Azure resources into Neo4j for deeper attack path and misconfiguration analysis.

This lab provides a practical understanding of Cirro's collection, ingestion, and analysis workflow. Attendees will perform enumeration and assessment of an Azure tenant to understand how to view attack paths beyond identities. They will perform Cypher queries and use custom dashboards to visualize and interpret graph data.

Prerequisites: - Docker/Podman Compose - Azure CLI - Web browser - Sqlite3 Browser Recommended (but not required): - Fundamental knowledge of Cypher query language

SpeakerBio: Leron Gray

Leron Gray is a Senior Security Consultant at Bishop Fox, specializing in offensive security, cloud attack path analysis, and security tooling research. He is the creator of Cirro, an extensible graph-based framework for analyzing Azure and cloud environments through Microsoft Graph and Azure Resource Manager data. His work focuses on helping security researchers and red teamers better understand complex cloud relationships, identity abuse paths, and infrastructure misconfigurations at scale.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Cloud Village - Friday - 14:30-15:10 PDT

Title: Citizen Developers Can't Defend What They Built: Scaling Security Past the Security Team

Tags: Cloud Village | Creator Talk/Panel

When: Friday, Aug 7, 14:30 - 15:10 PDT

Where: LVCCW Level 3 W313 (Cloud Village Talks) - [Map](#)

Description:



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Recon Village - Saturday - 15:30-15:59 PDT

Title: Cl0p ^_- Til You Drop - 6 years, 9 Campaigns, 7 0-Days

Tags: Recon Village | Creator Talk/Panel

When: Saturday, Aug 8, 15:30 - 15:59 PDT

Where: LVCCW Level 1 Hall 3 801 (Creator Stage 2) - [Map](#)

Description:

Cl0p has executed at least nine major exploitation campaigns since 2020, targeting file transfer and edge devices from Accellion to MOVEit to Centrestack. Each campaign looks different on the surface, different CVEs, different victims, different tooling. But their infrastructure tells a different story.

This talk presents the results of a multi-year infrastructure reconnaissance effort tracking Cl0p's hosting, ASN usage, and operational patterns across all known campaigns. By mining passive DNS data, network telemetry, and hosting records, I mapped the infrastructure behind each campaign and identified patterns the group can't seem to shake — including a favorite bulletproof hosting provider used across four separate campaigns, a finding that roughly one-third of their ASNs get recycled, and pre-attack reconnaissance probing observed as far as two years before exploitation.

SpeakerBio: Eli Woodward, Senior Threat Intelligence Advisor with Team Cymru

Eli Woodward is a cyber threat intelligence advisor with Team Cymru. He's worked in a variety of industries including financial services and government, and has seen the range of organizations from extremely well-resourced and capable to the shoestring budget. This has given him unique insights into CTI at all levels of complexity, maturity, and resources. He holds a master's degree in Intelligence and Security Studies and also plays bagpipes competitively.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Clash of Prompts: The World's First Prompt Battle Royale

Tags: AppSec Village | Creator Event/Activity

When: Friday, Aug 7, 11:00 - 12:59 PDT

Where: LVCCW Level 1 Hall 2 604 (Appsec Village) POD 3 - [Map](#)

Description:

Clash of Prompts is the world's first live, head-to-head AI prompt battle royale. Two developers tackle the same coding challenge, one prompt each, on the clock, while the AI generates the code live on screen. Every prompt is scored in real time on vulnerabilities, security best practices, and prompt efficiency.

Research shows 87-94% of AI-generated code ships with security flaws, even when developers try to prompt securely. This Pod is a hands-on way to see that play out: attendees write and test real prompts and watch them get scored instantly.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Clash of Prompts: The World's First Prompt Battle Royale

Tags: AppSec Village | Creator Event/Activity || All Audiences

When: Sunday, Aug 9, 11:00 - 12:59 PDT

Where: LVCCW Level 1 Hall 2 604 (Appsec Village) POD 1 - [Map](#)

Description:

Clash of Prompts is the world's first live, head-to-head AI prompt battle royale. Two developers tackle the same coding challenge, one prompt each, on the clock, while the AI generates the code live on screen. Every prompt is scored in real time on vulnerabilities, security best practices, and prompt efficiency.

Research shows 87-94% of AI-generated code ships with security flaws, even when developers try to prompt securely. This Pod is a hands-on way to see that play out: attendees write and test real prompts and watch them get scored instantly.

Speakers: Darren McNelis, Jerome Roberts

SpeakerBio: Darren McNelis

No BIO available

SpeakerBio: Jerome Roberts

With over 20 years of experience in cybersecurity and 15 years as a CxO, Jérôme has a proven track record in driving successful outcomes. He has been instrumental in five successful exits, including Lexsi (acquired by Orange in 2016) and Alsid (acquired by Tenable in 2021). Starting his career in deep-tech, mathematics, and engineering, Jérôme transitioned seamlessly into business leadership, leveraging his technical roots to guide strategic decisions and foster innovation in the cybersecurity landscape.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Lockpick Village - Saturday - 11:00-11:30 PDT

Title: Classic US High Sec: how to pick a Medeco

Tags: Lockpick Village | Creator Talk/Panel

When: Saturday, Aug 8, 11:00 - 11:30 PDT

Where: LVCCW Level 1 Hall 1 407 (Lockpick Village) - [Map](#)

Description:

With pins that both slide up and down and rotate, Medeco locks have been one of the most common high security locks in the US for over 50 years. Come learn exactly how they work, and how to open them with standard picks.

SpeakerBio: Max A

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Classical OSINT using AI (Actual Intelligence)

Tags: OSINT For Good Community | Creator Talk/Panel

When: Friday, Aug 7, 13:30 - 14:30 PDT

Where: LVCCW Level 1 Hall 3 1100 (Creator Stage 7) - [Map](#)

Description:

AI this, AI that, and of course even in the world of OSINT AI has been getting integrated. But this talk focuses on a different AI: Actual Intelligence. Modern investigators have access to more tools, automation, and artificial intelligence than ever before, yet many investigations still suffer from poor assumptions, weak validation, and information overload. Long before automated platforms and AI assistants existed, investigators relied on analytical thinking, source evaluation, and structured methodology to turn information into intelligence. This session introduces the ACTUAL framework. Through practical examples and real-world investigative scenarios, attendees will learn how to validate findings with confidence and conduct effective OSINT investigations even when specialized tools aren't available. Tools help collect information, but ACTUALLY intelligence comes from the investigator.

SpeakerBio: Bianca C. Ionescu/reconcerto

Bianca Ionescu is a CyberCorps SFS scholar pursuing a master's degree in cybersecurity at UNLV. She's served as a leader within cybersecurity student organizations, promoting growth, inclusion, and professional development. Her interests include open-source intelligence and mentoring new learners entering the field. Offline, she enjoys strength training and playing the viola. She's motivated by community building, continuous learning, and the challenge of solving complex security problems that inspire her growth and resilience every day.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Cleared for Takeoff: Debunking “Uncertifiable” Cybersecurity

Tags: Aerospace Village | Creator Talk/Panel

When: Friday, Aug 7, 15:30 - 15:59 PDT

Where: LVCCW Level 1 Hall 3 1103 (Creator Stage 5) - [Map](#)

Description:

Cybersecurity threats are rapidly becoming a first-order safety concern in critical aviation systems. Increasing in-flight connectivity, satellite communications, and networked avionics have eroded the assumption of airborne isolation. At the same time, AI-generated attacks are lowering both the barrier to entry and the time-to-exploit, enabling faster, more adaptive threat behavior. In contrast, patching and remediation time in aviation systems remains long due to rigorous certification and deployment constraints. This growing asymmetry further elevates cybersecurity risk into a direct safety concern. In this environment, a security risk is a safety risk. This raises a critical question: not whether cybersecurity is needed in aircraft, but whether cybersecurity tools can be certified for safety-critical airborne systems.

This talk focuses on the challenge of bridging that gap by asking: can we generate the right verification artifacts to make existing cybersecurity tools certifiable, without modifying their core functionality? We explore why cybersecurity tools are rarely introduced into DAL-A airborne systems in their native form, focusing on the mismatch between operational security outputs and certification evidence requirements. The core problem is not only deterministic behavior, but the lack of structured, complete, and traceable artifacts to support certification arguments.

SpeakerBio: Katie Fejer

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Clew: Untangling Evasive Malware with Per-Sample Fuzzing Seeds

Tags: DEF CON Demo Labs | Intermediate | Defense/Blue Team | Malware | DEF CON Demo Labs

When: Saturday, Aug 8, 11:00 - 11:45 PDT

Where: LVCCW Level 1 Hall 3 1003 (Demo Labs Track 3) - [Map](#)

Description:

Clew is an automated fuzzing-candidate extraction pipeline for environment-sensitive malware analysis. Evasive malware routinely queries its execution environment via Windows API calls to hide functionality until specific environmental conditions are met. By hooking these API calls, a fuzzer can reveal such execution paths that are typically hidden during standard analysis. No seed corpus of environmental fuzzing candidates currently exists for this application. As a result, current API-hooking fuzzers rely on hand-written, sample-agnostic starting values and blind mutations that cannot scale to the diverse evasion techniques seen in sophisticated samples. Clew addresses this by analyzing each PE32 binary and producing a per-sample seed corpus of candidate API return values that downstream environmental fuzzers use to systematically uncover hidden execution paths.

Speakers: Kyler McElroy, Anita Ding, Daniel Koranek

SpeakerBio: Kyler McElroy

McElroy, a second lieutenant and developmental engineer in the United States Air Force, is pursuing a master's in computer science with an AI focus at the Air Force Institute of Technology. His research focuses on using machine learning and automated analysis to uncover hidden behaviors in evasive malware. He is an alumnus of the ACE Cyber Leadership Development program, where he authored S.A.N.D (Synthetic Adversarial and Natural Data Generation) under the Air Force Research Laboratory.

SpeakerBio: Anita Ding

Anita Ding is a second lieutenant and cyber operations officer in the United States Air Force, is pursuing a master's in cyber operations with an AI focus at the Air Force Institute of Technology. Her research focuses on LLM-orchestrated red team automation and graph neural networks for attack-path scoring in Active Directory environments. She earned a B.A. in Computer Science from UC Berkeley, where she conducted research at the Berkeley AI Research Lab and the Berkeley Risk and Security Lab. She is also an alumna of the ACE Cyber Leadership Development program, where she designed a CTF challenge for the British Army's Defence Cyber Marvel exercise.

SpeakerBio: Daniel Koranek

Dr. Daniel Koranek is an Assistant Professor of Computer Science at the Air Force Institute of Technology (AFIT) and a two-time graduate of AFIT in cyber operations (2010, M.S.) and computer science (2022, Ph.D.), where his research interests focus on the intersection of artificial intelligence/machine learning and cybersecurity. This includes using AI/ML to enhance cybersecurity and using vulnerability assessment and secure design techniques to improve AI deployments. He has spent most of his career on reverse engineering and vulnerability assessment of embedded systems, and overlapping AI and cybersecurity drove Dr. Koranek's dissertation research on using the reverse engineering tool Binary Ninja to visualize explanations of malware classifications.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Clew: Untangling Evasive Malware with Per-Sample Fuzzing Seeds

Tags: DEF CON Demo Labs | Intermediate | Defense/Blue Team | Malware | DEF CON Demo Labs

When: Friday, Aug 7, 14:00 - 14:45 PDT

Where: LVCCW Level 1 Hall 3 1003 (Demo Labs Track 3) - [Map](#)

Description:

Clew is an automated fuzzing-candidate extraction pipeline for environment-sensitive malware analysis. Evasive malware routinely queries its execution environment via Windows API calls to hide functionality until specific environmental conditions are met. By hooking these API calls, a fuzzer can reveal such execution paths that are typically hidden during standard analysis. No seed corpus of environmental fuzzing candidates currently exists for this application. As a result, current API-hooking fuzzers rely on hand-written, sample-agnostic starting values and blind mutations that cannot scale to the diverse evasion techniques seen in sophisticated samples. Clew addresses this by analyzing each PE32 binary and producing a per-sample seed corpus of candidate API return values that downstream environmental fuzzers use to systematically uncover hidden execution paths.

Speakers: Kyler McElroy, Anita Ding, Daniel Koranek

SpeakerBio: Kyler McElroy

McElroy, a second lieutenant and developmental engineer in the United States Air Force, is pursuing a master's in computer science with an AI focus at the Air Force Institute of Technology. His research focuses on using machine learning and automated analysis to uncover hidden behaviors in evasive malware. He is an alumnus of the ACE Cyber Leadership Development program, where he authored S.A.N.D (Synthetic Adversarial and Natural Data Generation) under the Air Force Research Laboratory.

SpeakerBio: Anita Ding

Anita Ding is a second lieutenant and cyber operations officer in the United States Air Force, is pursuing a master's in cyber operations with an AI focus at the Air Force Institute of Technology. Her research focuses on LLM-orchestrated red team automation and graph neural networks for attack-path scoring in Active Directory environments. She earned a B.A. in Computer Science from UC Berkeley, where she conducted research at the Berkeley AI Research Lab and the Berkeley Risk and Security Lab. She is also an alumna of the ACE Cyber Leadership Development program, where she designed a CTF challenge for the British Army's Defence Cyber Marvel exercise.

SpeakerBio: Daniel Koranek

Dr. Daniel Koranek is an Assistant Professor of Computer Science at the Air Force Institute of Technology (AFIT) and a two-time graduate of AFIT in cyber operations (2010, M.S.) and computer science (2022, Ph.D.), where his research interests focus on the intersection of artificial intelligence/machine learning and cybersecurity. This includes using AI/ML to enhance cybersecurity and using vulnerability assessment and secure design techniques to improve AI deployments. He has spent most of his career on reverse engineering and vulnerability assessment of embedded systems, and overlapping AI and cybersecurity drove Dr. Koranek's dissertation research on using the reverse engineering tool Binary Ninja to visualize explanations of malware classifications.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Bug Bounty Village - Friday - 10:00-10:30 PDT

Title: Click Me: Turning URI Links into Bug Bounty RCE's

Tags: Bug Bounty Village | Creator Talk/Panel

When: Friday, Aug 7, 10:00 - 10:30 PDT

Where: LVCCW Level 2 W206-207 (Bug Bounty Village) - [Map](#)

Description:

Bug bounty hunters often encounter unprotected URL inputs and dismiss them as low-impact findings. This presentation explores real-world Microsoft enterprise application vulnerabilities where custom URI handlers led to remote code execution. Attendees will learn how pivoting from web applications into desktop software can reveal impactful attack paths hidden behind seemingly mundane bugs.

SpeakerBio: Tobias Diehl

Tobias Diehl is a Senior Offensive Security Engineer, security researcher, and Microsoft 2025 Most Valuable Researcher (MVR) specializing in offensive security, enterprise AI, bug bounty research, and adversary emulation. His work focuses on identifying overlooked attack paths where web applications, AI systems, and desktop software intersect, helping organizations understand how seemingly low-risk vulnerabilities can become high-impact security issues. Tobias leads offensive security assessments, conducts purple team exercises, and performs research into emerging attack techniques affecting enterprise environments. His work has resulted in multiple security findings impacting Microsoft technologies, including Power Platform, CoPilot and other AI-driven applications. A returning DEF CON speaker, Tobias is passionate about sharing practical research that helps both security researchers and defenders better understand modern attack chains. His presentations emphasize real-world case studies, responsible disclosure, and actionable defensive guidance for securing the next generation of AI-enabled enterprise systems.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Clone to Pwn: Remote Badge Cloning with the Flipper Zero

Tags: Physical Security Village | Creator Talk/Panel

When: Saturday, Aug 8, 14:00 - 14:59 PDT

Where: LVCCW Level 1 Hall 3 1104 (Creator Stage 4) - [Map](#)

Description:

Traditional RFID badge cloning methods require you to be within 3 feet of your target. So how can you conduct a physical penetration test and clone a badge without interacting with a person? Companies have increasingly adopted a hybrid work environment, allowing employees to work remotely, which has decreased the amount of foot traffic in and out of a building at any given time. This session discusses two accessible, entry-level hardware designs you can build in a day and deploy in the field, along with the tried-and-true social engineering techniques that can increase your chances of remotely cloning an RFID badge.

Langston and Dan discuss their Red Team adventures using implant devices and their Flipper Zero workflow. As a bonus the two will present a new python script to help you decode your badge data faster. This presentation is supplemented with files and instructions that are available for download in order to build your own standalone gooseneck reader, wall implant and clipboard cloning devices!

Speakers:Langston Clement,Dan Goga

SpeakerBio: Langston Clement, Security Risk Advisors (SRA)

Langston grew up reading stories about the 90's hacker escapades, and after years of observing the scene, he jumped into the offensive security field and never looked back. He is currently a Senior Purple Team Advisor for Security Risk Advisors (SRA). With over fifteen (15) years of public and private sector experience in cybersecurity and ethical hacking, he aims to provide organizations with valuable and actionable information to help improve their security posture. Langston's specializations focus on modern-day social engineering techniques, wireless and RFID attacks, red teaming, physical penetration testing and purple team engagements.

SpeakerBio: Dan Goga, Principal Consultant at NRI North America

Dan Goga serves as a Principal Consultant with NRI focused on conducting penetration testing and red team assessments. Dan Goga has nine years of information security experience in the public, private, and academic sectors. Dan has extensive knowledge and experience with RFID hacking, phishing techniques, social engineering techniques, and penetration testing.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Cloud Village - Sunday - 13:10-13:30 PDT

Title: Closing Talk

Tags: Cloud Village | Creator Talk/Panel

When: Sunday, Aug 9, 13:10 - 13:30 PDT

Where: LVCCW Level 3 W313 (Cloud Village Talks) - [Map](#)

Description:

SpeakerBio: Jayesh Singh Chauhan

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Cloud Forensics 101 : Ghost in the logs

Tags: Blue Team Village | Creator Talk/Panel

When: Saturday, Aug 8, 12:00 - 12:59 PDT

Where: LVCCW Level 2 W217 (Blue Team Village) Main Stage - [Map](#)

Description:

Cloud breaches don't look like Hollywood hacking; they look like a leaked API key and a bot finding it before you've finished your coffee. This introduction to cloud forensics talk walks through a real AWS attack path end-to-end: recon, initial access, privilege escalation, exfiltration, and impact. We'll cover the misconfigurations that actually get exploited in the wild, how to contain them, and close with a demo: a deliberately compromised AWS account, investigated using AI to turn raw CloudTrail logs into a clean incident timeline in minutes.

Speakers: Cassandra (muteki) Young, Dimple Gajra

SpeakerBio: Cassandra (muteki) Young

As a Principal Consultant on [REDACTED]'s Cloud Technical Advisory team, muteki analyzes the organizational security posture of Azure, GCP and Oracle Cloud environments, and leads the development of data collection and analysis tooling. Additionally, she assists the Incident Response team as a technical GCP and OCI SME, and supports strategic advisory and technical tabletop exercises across multiple cloud platforms. In addition to her decade of IT and then cloud security consulting experience, muteki also holds a Master's in Computer Science and is a director of Blue Team Village, a nonprofit organization bringing free Blue Team content to the community.

SpeakerBio: Dimple Gajra

Specializing in Digital Forensics, Incident Response (DFIR), and privacy engineering, Dimple Gajra (aka LocalHost) brings technical expertise to enterprise defense and data protection. Her professional journey includes engineering and response roles at major technology enterprises like IBM and Amazon's Security Incident Response Team (SIRT), where she has actively defended critical infrastructure, mitigated high-severity ransomware incidents, and engineered solutions to safeguard data privacy and automate secure detection pipelines. Driven by a hands-on, analytical approach to uncovering adversary tradecraft, she focuses on building architectural resilience, protecting sensitive user data, and translating complex system artifacts into actionable defensive strategies.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Cloud Village CTF: Three Azure Warmups

Tags: DCNextGen | Creator Event/Activity | Youth

When: Sunday, Aug 9, 10:00 - 10:59 PDT

Where: LVCCW Level 3 W316 (DC NextGen) - [Map](#)

Description:

Welcome to Apex Park, where cloud-security mistakes are causing trouble throughout the park! Participants will investigate three beginner-friendly Azure challenges involving an exposed gift shop, an overpowered day pass, and an unlocked control room. They will inspect websites, investigate cloud-storage permissions, follow clues, and recover hidden flags. No access to a real Azure account or the challenge infrastructure is required. Participants interact only with intentionally vulnerable CTF resources created for learning.

SpeakerBio: Cloud Village

No BIO available

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

The Diana Initiative - Friday - 13:00-13:10 PDT

Title: Cloud Village Tour

Tags: The Diana Initiative | Creator Tour

When: Friday, Aug 7, 13:00 - 13:10 PDT

Where: LVCCW Level 1 South Lobby / Atrium - [Map](#)

Description:

Interested in visiting Cloud Village but afraid to go by yourself? The Diana Initiative is hosting tours! Follow a volunteer to Cloud Village and be introduced to the community and activities inside!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: cloud-auth: a provider-agnostic CLI for cross-cloud workload identity

Tags: Demo | Cloud Village | Creator Talk/Panel

When: Saturday, Aug 8, 14:50 - 15:20 PDT

Where: LVCCW Level 3 W313 (Cloud Village Talks) - [Map](#)

Description:

Modern engineering teams don't live in one cloud. A workload in Google Kubernetes Engine needs to read from an S3 bucket. An EC2 instance needs to fetch a secret from Azure Key Vault. A single GitHub Actions job has to deploy to AWS, log telemetry to GCP, and trigger a workflow in Azure — all in the same run. The default way teams make this work is the same way they have for a decade: paste a long-lived credential into a secret and hope nobody finds it.

This is the credential sprawl problem at the heart of every multi-cloud breach. Static AWS access keys, GCP service account JSON files, Azure client secrets — the most reliably exploited foothold in cloud environments, sitting in env vars, secret managers, and committed git history across every blue team's environment.

Why this was hard before cloud-auth? In theory, every major cloud already supports a way to skip the static credential entirely. A GKE pod can assume an AWS IAM role directly — no AWS keys anywhere. An EC2 instance can call Azure with no service principal on it. A Kubernetes workload can hit GCP APIs with no service account JSON file. In practice, each cloud has its own model, API, and failure modes. Setting up just one of these connections means learning a new mental model, authoring trust documents with provider-specific subject formats, and validating it all by hand. Doing it across clouds means doing that work three or four times over, with no consistent way to set it up, validate it, or clean it up. That friction is why cloud-auth exists. The secure path is already supported by the clouds — defenders just need tooling that makes it as easy as pasting an access key, or easier. So most teams stay on static keys.

cloud-auth: cross-cloud workload identity for defenders cloud-auth is an open-source CLI and library that gives blue teams one consistent way to set up, validate, and safely retire cross-cloud workload identity. One command stands up the trust between any two of: AWS, GCP, Azure, HashiCorp Vault, Cloudflare, GitHub Actions, and Kubernetes. The same command validates it, previews changes before applying, and tears it down without touching anything it didn't create.

Live demo GKE pod → AWS S3, no AWS keys. A GKE pod reads from S3 using a short-lived AWS role. EC2 → Azure Key Vault, no service principal. An EC2 instance fetches a secret with no Azure client secret on it. GitHub Actions → AWS, GCP, and Azure in one workflow. A single CI job deploys across three clouds. Catching a misconfigured trust. The validator flags an overly permissive trust before it ships. Safe teardown. Dry-run a multi-cloud cleanup, then execute. cloud-auth only deletes what it created.

What attendees leave with? A working open-source tool, a concrete pattern for cross-cloud workload identity, and a validation framework to drop into existing CI/CD. Repository: <https://github.com/anirudhbiyani/cloud-auth> (LGPL-3.0)

SpeakerBio: Aniruddha Biyani

Aniruddha "AB" Biyani leads the Security and Compliance program at Prophecy, where he focuses on building security as a business enabler for high-growth cloud and AI platforms. His work centers on scaling information security programs, strengthening cloud and identity security, enabling secure product development, and aligning security strategy with customer trust, compliance, and engineering velocity. He has previously held security roles at Mandiant, Securonix, CRED, and Khoros.

AB's career spans cloud security leadership across startups and cybersecurity vendors, with deep experience in defensive cloud engineering, identity and access management, secure developer enablement, and operationalising secure-by-default practices in fast-moving organizations. He is known for translating complex security challenges into practical programs, tools, and frameworks that help engineering teams move quickly while reducing risk.

AB has presented at global security conferences including Black Hat Arsenal, SANS CloudSecNext, and MCPDev BLR, on workload identity, multi-cloud attack surface discovery, credential lifecycle management, and secure cloud adoption at scale. He is also an active open-source contributor and community builder, maintaining cloud security tools and secure developer training resources. He previously served for three years as a core DEF CON Cloud Village CTF volunteer, leading contest design and build efforts.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Cloud-Native C2: Weaponizing Trusted Infrastructure for Initial Access

Tags: Red Team Village | Misc

When: Friday, Aug 7, 14:00 - 15:59 PDT

Where: LVCCW Level 1 Hall 1 309 (Red Team Village) Tactic Table 1 - [Map](#)

Description:

Traditional command and control infrastructure faces constant detection pressure from network defenders. This research presents two novel proof-of-concept frameworks that demonstrate how seemingly benign cloud services can be weaponized for covert operations. MeetC2 leverages Google Calendar API to transform calendar events into a bidirectional C2 channel, while XRayC2 repurposes AWS X-Ray's distributed tracing service for command execution and data exfiltration.

Both frameworks exploit fundamental assumptions about trusted services: calendar synchronization traffic appears as routine business operations, while X-Ray traces blend seamlessly with legitimate application monitoring. Our implementations showcase practical techniques including command encoding in calendar event metadata, response embedding in trace annotations, and beacon patterns that mimic normal service behavior. The frameworks support cross-platform implants with minimal footprint, requiring only API credentials rather than traditional malware persistence.

I will demonstrate how these channels bypass traditional security controls, as encrypted HTTPS traffic to Google and AWS endpoints rarely triggers alerts. The research reveals critical blind spots in cloud security monitoring and provides actionable detection strategies, including API usage anomalies, unusual trace patterns, and calendar event behavioral analysis. This work aims to help defenders understand emerging cloud-native threats and implement appropriate monitoring for their cloud environments.

As organizations increasingly adopt cloud services, attackers have evolved their tactics to abuse these trusted platforms for malicious purposes. Cloud service APIs present an attractive option for establishing command and control infrastructure because they offer high availability, encrypted communications by default, and traffic that blends with legitimate business operations. This research explores how adversaries can weaponize standard cloud APIs to create sophisticated C2 channels that circumvent traditional security controls.

This research presents two functional C2 frameworks for initial access that abuse legitimate cloud APIs: MeetC2 leveraging Google Calendar for command and control, and XRayC2 weaponizing AWS X-Ray distributed tracing.

SpeakerBio: Dhiraj Mishra

An active speaker who has discovered multiple zero-days in modern web browsers and an open-source contributor. He is a trainer at Blackhat, BruCON, 44CON and presented in conferences such as Ekoparty, NorthSec, Hacktivity, PHDays, Hack in Paris & HITB. In his free time, he blogs at www.inputzero.io/www.fuzzing.at and tweets on @RandomDhiraj.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: CloudBashing: Exploiting free CloudShells for mining, networking, exfil, and persistence at scale

Tags: DEF CON Official Talk | Demo | Tool

When: Friday, Aug 7, 16:30 - 17:30 PDT

Where: LVCCW Level 1 Hall 3 904 (Main Track 4) - [Map](#)

Description:

CloudBashing started with reversing the private AWS, Azure, and GCP CloudShell REST and websocket terminal protocols, then tracing and analyzing janky browser authentication/credential flows from cookies to OAuth tokens. Along the way, we automated the APIs to access free CPU/networking, maintained access across container/VM resets, utilized persistent \$HOME for implants/data, locked users out of sudo access, and installed a C2 framework. We discovered IAM design issues like: AWS role assumption that result in a large # of environments per compromised identity, web socket sessions that survive API token revocation, and M365/Gmail consumer email accounts that have default CloudShell access. This turned into a newly released exploit toolkit, CloudBasher, that enumerates, validates, installs, and runs distributed workloads with virtual storage and private networking across a large-scale agent network with persistence and resilience. We'll demo distributing CPU-intensive workloads, using virtual storage for staging/exfiltration, secure networking for proxy and obfuscated exfil paths, while automating the discovery, enumeration, creation of CloudShell environments from initial credentials/sessions to implants/setup/networking to management and control.

Amazon Web Services, "AWS CloudShell service authorization reference,"

https://docs.aws.amazon.com/service-authorization/latest/reference/list_awscloudshell.html

Amazon Web Services, "AWS Systems Manager StartSession API (SSM framing basis),"

https://docs.aws.amazon.com/systems-manager/latest/APIReference/API_StartSession.html

Google Cloud, "Cloud Shell API v1 REST reference,"

<https://docs.cloud.google.com/shell/docs/reference/rest/v1/users.environments>

Microsoft Azure, "Azure Cloud Shell overview," <https://docs.microsoft.com/en-us/azure/cloud-shell/overview>

OSRU @ ronin.ae, "AWS CloudShell analysis: privileged container, exposed block devices and container escape(s)," October 23, 2023, <https://web.archive.org/web/20240912135502/https://ronin.ae/news/aws-cloudshell-analysis/>

Aidan Steele, "Deep dive into AWS CloudShell," awsteele.com, January 11, 2024,

<https://awsteele.com/blog/2024/01/11/deep-dive-into-aws-cloudshell.html>

Paul Schwarzenberger, "CloudShell slip-up: command-line access to underlying AWS infrastructure," Medium, October 15, 2024,

<https://medium.com/@paulschwarzenberger/cloudshell-slip-up-command-line-access-to-underlying-aws-infrastructure-ae77a08580>

Rhino Security Labs, "AWS CloudShell Lateral Movement," <https://rhinosecuritylabs.com/aws/cloudshell-lateral-movement/>

Eduard Agavriiloae, "notyet: AWS IAM Credential Revocation Gaps," offensai,

<https://www.offensai.com/blog/notyet-aws-iam-credential-revocation-gaps>

Dan Vittegleo, cloudshell-store, GitHub Repository, <https://github.com/dan-v/cloudshell-store>

FrancescoDiSalesGithub, "Google-cloud-shell-hacking," GitHub Repository,

<https://github.com/FrancescoDiSalesGithub/Google-cloud-shell-hacking>

Bipin Jitiya, "Google Cloud Shell Container Escape," Medium, December 14, 2025,
<https://medium.com/@win3zz/google-cloud-shell-container-escape-b69ffb46b5df>

Bertrand Martel, "AWS SSM Session: JavaScript library for AWS Systems Manager Session Manager," GitHub,
<https://github.com/bertrandmartel/aws-ssm-session>

Amazon Web Services, "Amazon SSM Agent: agentmessage.go," AWS GitHub Repository,
<https://github.com/aws/amazon-ssm-agent/blob/c65d8ac29a8bbe6cd3f7cea778c1eeb1b06d49a3/agent/session/contracts/agentmessage.go>

SentinelOne, "CVE-2026-32169: Azure Cloud Shell SSRF Vulnerability," SentinelOne Vulnerability Database, March 19, 2026, <https://www.sentinelone.com/vulnerability-database/cve-2026-32169/>

Speakers:Jenko "edleft" Hwong,Chris Ryan

SpeakerBio: Jenko "edleft" Hwong, Huntress Labs

Jenko Hwong is a Principal Security Researcher at Huntress Labs, focusing on identity-based attacks and cloud abuse. Prior to Huntress, he spent 6 years at Netskope Threat Labs, has spoken at RSA and DEFCON, and is a Cloud Village Lead. He has over 20 years at various security startups in cloud detection/response, vulnerability scanning, AV/AS, pen-testing/exploits, L3/4 appliances, threat intel, and windows security.

SpeakerBio: Chris Ryan, Huntress Labs

A series of oddly configured server banners, a JARM fingerprint, curious fields in a security certificate - these aren't just technical details, but are instead threads in a narrative tapestry woven like a John le Carre novel. For over 20 years, Chris has dedicated his life to studying these threads and the intersection between cybersecurity, Russian linguistics, and free and open source software. His career path has taken detours through academia, aerospace and defense, software development, and cybersecurity.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Cloudy with a Chance of Breaches: Hands-On AWS Threat Defense

Tags: Cloud Village | Creator Event/Activity | Investigation

When: Friday, Aug 7, 13:30 - 15:30 PDT

Where: LVCCW Level 3 W311 (Cloud Village Labs) A - [Map](#)

Description:

Join this hands-on workshop to explore integrated security capabilities for the modern AWS cloud stack, including containers, object storage, and AI applications. You'll work with a deliberately vulnerable Flask application running on EKS with S3 and Amazon Bedrock, then deploy and configure controls that detect attacks at runtime.

The session will cover behavioral runtime detection for credential-access activity and malware inside live pods, attack-surface mapping, and identity-aware risk analysis to trace the potential blast radius of a compromised workload through its IAM role. You'll also examine file-borne threat protection across the application boundary and S3, use unified XDR queries to hunt across container and storage detections, and close with runtime guardrails that block direct and document-borne prompt injection against a real Amazon Bedrock model.

SpeakerBio: Kyle Hubbard

Kyle is a Solutions Architect at TrendAI, where he works within the Global Alliances team across hyperscaler partnerships, with a primary focus on AWS. He specializes in cloud security integrations and in translating the technical capabilities of the Trend Vision One platform into strategies that partners, customers, and executives can act on.

His current work is centered on AI security, including AI security posture management and the protection of agentic workloads. As organizations rapidly adopt agentic architectures, Kyle focuses on how Vision One can secure that transition and how to communicate its value clearly to both technical and executive audiences.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Cloudy with a Chance of Venting: Managing Supply Chain Risk

Tags: Blue Team Village | Creator Talk/Panel

When: Friday, Aug 7, 17:00 - 17:59 PDT

Where: LVCCW Level 2 W217 (Blue Team Village) Main Stage - [Map](#)

Description:

As organizations scale across a fragmented mix of SaaS, PaaS, and hyperscale environments, the enterprise attack surface is no longer fully under their control. Today's threat actors aren't just targeting the cloud, they are weaponizing the cloud supply chain and exploiting these new dependencies. Bringing together diverse practitioner perspectives, this panel addresses the hard operational questions of modern cloud security.

Our experts will break down the structural differences in evaluating risk across various cloud tiers, share proactive blueprints for hardening application supply chains, and debate the unique pitfalls of executing incident response when a critical SaaS provider or cloud asset is compromised.

Speakers: Cassandra (muteki) Young, Christian Nicholson, David Collins, Kyle Dickinson, Ricky (0xpsilocyber) Banda

SpeakerBio: Cassandra (muteki) Young

As a Principal Consultant on [REDACTED]'s Cloud Technical Advisory team, muteki analyzes the organizational security posture of Azure, GCP and Oracle Cloud environments, and leads the development of data collection and analysis tooling. Additionally, she assists the Incident Response team as a technical GCP and OCI SME, and supports strategic advisory and technical tabletop exercises across multiple cloud platforms. In addition to her decade of IT and then cloud security consulting experience, muteki also holds a Master's in Computer Science and is a director of Blue Team Village, a nonprofit organization bringing free Blue Team content to the community.

SpeakerBio: Christian Nicholson

Christian is a recognized technology leader specializing in cloud architectures and secure-by-design implementation. Maintaining deep technical expertise, Christian bridges the gap between IT, business teams, and users. A global speaker, advisor, and organizer for major IT and security conferences and global events, Christian also contributes to international policy through United Nations (UN) and global policy dialogues to shape secure digital ecosystems.

SpeakerBio: David Collins

Dave works to secure modern infrastructure and applications, with a focus on cloud-deployed systems.

SpeakerBio: Kyle Dickinson

Kyle D is a professional overthinker who's spent years securing complex systems at scale without killing the fun. A former Threat Detection and Response specialist at {Cloud Provider Here}, he now lives at the intersection of cloud, gaming, and security.

SpeakerBio: Ricky (0xpsilocyber) Banda

Hi!

I am a incident responder with over 15 years of experience with a focus on incident management. I have worked at orgs from USAF, to Amazon, to Google, and have responded to a wide array of threats across the industry. Feel free to say hi after the



Contests - Sunday - 10:00-12:59 PDT

Title: CMD+CTRL Cyber Range: DarkMoney

Tags: CMD+CTRL Cyber Range | Contest

When: Sunday, Aug 9, 10:00 - 12:59 PDT

Where: LVCCW Level 1 Hall 1 405 (CMD+CTRL Cyber Range) - [Map](#)

Description:

CMD+CTRL is back for our 10th year and bringing something new to show. Drop by our cyber range for hands-on web application security challenges designed for all skill levels. Come to learn, come to compete, come to break things. All are welcome, whether it's your 1st CTF or your 101st.

There is no pre-qualification, and the only participant prerequisite is "Computer with internet access."

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Contests - Saturday - 10:00-17:59 PDT

Title: CMD+CTRL Cyber Range: DarkMoney

Tags: CMD+CTRL Cyber Range | Contest

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 405 (CMD+CTRL Cyber Range) - [Map](#)

Description:

CMD+CTRL is back for our 10th year and bringing something new to show. Drop by our cyber range for hands-on web application security challenges designed for all skill levels. Come to learn, come to compete, come to break things. All are welcome, whether it's your 1st CTF or your 101st.

There is no pre-qualification, and the only participant prerequisite is "Computer with internet access."



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Contests - Friday - 10:00-17:59 PDT

Title: CMD+CTRL Cyber Range: DarkMoney

Tags: CMD+CTRL Cyber Range | Contest

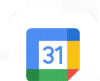
When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 405 (CMD+CTRL Cyber Range) - [Map](#)

Description:

CMD+CTRL is back for our 10th year and bringing something new to show. Drop by our cyber range for hands-on web application security challenges designed for all skill levels. Come to learn, come to compete, come to break things. All are welcome, whether it's your 1st CTF or your 101st.

There is no pre-qualification, and the only participant prerequisite is "Computer with internet access."



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Contests - Saturday - 10:00-17:59 PDT

Title: Code Cadaver: Break Every System. Save Your Friend.

Tags: Biohacking Village | Code Cadaver (Biohacking Village CTF) | Contest

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 306 (Biohacking Village CTF: Code Cadaver) - [Map](#)

Description:

Biohacking Village Capture the Flag: Test your skills against healthcare-themed capture the flag challenges. From beginner to expert levels, there's something for everyone.

Code Cadaver: Break Every System. Save Your Friend.

Your best friend entered St. Dismas Hospital with flu-like symptoms.

He never came back.

Now his hotel room has been torn apart, his phone is still beaconing somewhere in the wreckage, and every clue points toward a hospital that seems less interested in healing people than hiding what happens to them.

Code Cadaver is Biohacking Village's immersive healthcare cybersecurity CTF—a dark, story-driven challenge that pulls players through the connected systems of a compromised hospital and the criminal network surrounding it.

Follow wireless signals. Pivot from guest networks into production systems. Hunt through patient intake records, webcams, HL7 traffic, payment systems, RFID credentials, pager networks, infusion devices, DICOM archives, and secured medical cabinets. Every system holds another piece of the truth. Every solved challenge brings you closer to Ethan—and deeper into St. Dismas.

This is more than a collection of puzzles. It is a full-chain medical cyber-thriller built around the technologies, mistakes, dependencies, and trust relationships that keep modern healthcare running.

You will need technical skill, persistence, curiosity, and a willingness to question everything.

The hospital is closing in.

The machines are still working.

Ethan is running out of time.

Break every system. Save your friend before St. Dismas finishes what it started.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Contests - Sunday - 10:00-13:59 PDT

Title: Code Cadaver: Break Every System. Save Your Friend.

Tags: Biohacking Village | Code Cadaver (Biohacking Village CTF) | Contest

When: Sunday, Aug 9, 10:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 1 306 (Biohacking Village CTF: Code Cadaver) - [Map](#)

Description:

Biohacking Village Capture the Flag: Test your skills against healthcare-themed capture the flag challenges. From beginner to expert levels, there's something for everyone.

Code Cadaver: Break Every System. Save Your Friend.

Your best friend entered St. Dismas Hospital with flu-like symptoms.

He never came back.

Now his hotel room has been torn apart, his phone is still beaconing somewhere in the wreckage, and every clue points toward a hospital that seems less interested in healing people than hiding what happens to them.

Code Cadaver is Biohacking Village's immersive healthcare cybersecurity CTF—a dark, story-driven challenge that pulls players through the connected systems of a compromised hospital and the criminal network surrounding it.

Follow wireless signals. Pivot from guest networks into production systems. Hunt through patient intake records, webcams, HL7 traffic, payment systems, RFID credentials, pager networks, infusion devices, DICOM archives, and secured medical cabinets. Every system holds another piece of the truth. Every solved challenge brings you closer to Ethan—and deeper into St. Dismas.

This is more than a collection of puzzles. It is a full-chain medical cyber-thriller built around the technologies, mistakes, dependencies, and trust relationships that keep modern healthcare running.

You will need technical skill, persistence, curiosity, and a willingness to question everything.

The hospital is closing in.

The machines are still working.

Ethan is running out of time.

Break every system. Save your friend before St. Dismas finishes what it started.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Contests - Friday - 10:00-17:59 PDT

Title: Code Cadaver: Break Every System. Save Your Friend.

Tags: Biohacking Village | Code Cadaver (Biohacking Village CTF) | Contest

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 306 (Biohacking Village CTF: Code Cadaver) - [Map](#)

Description:

Biohacking Village Capture the Flag: Test your skills against healthcare-themed capture the flag challenges. From beginner to expert levels, there's something for everyone.

Code Cadaver: Break Every System. Save Your Friend.

Your best friend entered St. Dismas Hospital with flu-like symptoms.

He never came back.

Now his hotel room has been torn apart, his phone is still beaconing somewhere in the wreckage, and every clue points toward a hospital that seems less interested in healing people than hiding what happens to them.

Code Cadaver is Biohacking Village's immersive healthcare cybersecurity CTF—a dark, story-driven challenge that pulls players through the connected systems of a compromised hospital and the criminal network surrounding it.

Follow wireless signals. Pivot from guest networks into production systems. Hunt through patient intake records, webcams, HL7 traffic, payment systems, RFID credentials, pager networks, infusion devices, DICOM archives, and secured medical cabinets. Every system holds another piece of the truth. Every solved challenge brings you closer to Ethan—and deeper into St. Dismas.

This is more than a collection of puzzles. It is a full-chain medical cyber-thriller built around the technologies, mistakes, dependencies, and trust relationships that keep modern healthcare running.

You will need technical skill, persistence, curiosity, and a willingness to question everything.

The hospital is closing in.

The machines are still working.

Ethan is running out of time.

Break every system. Save your friend before St. Dismas finishes what it started.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Code Invaders: Stop The Insecure Code

Tags: AppSec Village | Creator Event/Activity | All Audiences

When: Saturday, Aug 8, 11:00 - 12:59 PDT

Where: LVCCW Level 1 Hall 2 604 (Appsec Village) POD 1 - [Map](#)

Description:

Recruit: help stop the Vibe Invasion. AI-generated code is flooding the frontier with insecure logic, and it's your job to intercept it before it hits production. Vulnerable snippets (SQL injections, hardcoded secrets, broken crypto, and risky error handling) are falling toward the pipeline. Eliminate the threats, but stay sharp: secure code is mixed in. One wrong move could cause damage. Defend production and stop the Vibe Coding Invasion.

SpeakerBio: Mackenzie

Mackenzie is a developer advocate with a passion for DevOps and code security. As the co-founder and former CTO of a health tech startup, he learnt first-hand how critical it is to build secure applications with robust developer operations.

Today as the Developer Advocate at GitGuardian, Mackenzie is able to share his passion for code security with developers and works closely with research teams to show how malicious actors discover and exploit vulnerabilities in code.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Code Invaders: Stop The Insecure Code

Tags: AppSec Village | Creator Event/Activity || All Audiences

When: Saturday, Aug 8, 13:00 - 14:59 PDT

Where: LVCCW Level 1 Hall 2 604 (Appsec Village) POD 1 - [Map](#)

Description:

Recruit: help stop the Vibe Invasion. AI-generated code is flooding the frontier with insecure logic, and it's your job to intercept it before it hits production. Vulnerable snippets (SQL injections, hardcoded secrets, broken crypto, and risky error handling) are falling toward the pipeline. Eliminate the threats, but stay sharp: secure code is mixed in. One wrong move could cause damage. Defend production and stop the Vibe Coding Invasion.

SpeakerBio: Mackenzie

Mackenzie is a developer advocate with a passion for DevOps and code security. As the co-founder and former CTO of a health tech startup, he learnt first-hand how critical it is to build secure applications with robust developer operations.

Today as the Developer Advocate at GitGuardian, Mackenzie is able to share his passion for code security with developers and works closely with research teams to show how malicious actors discover and exploit vulnerabilities in code.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Code to Cloud: Secure Modern Applications Using Open-Source Tools

Tags: Intermediate | AppSec Village | Creator Workshop

When: Saturday, Aug 8, 16:15 - 17:59 PDT

Where: LVCCW Level 1 Hall 2 604 (Appsec Village) Classroom - [Map](#)

Description:

Want to build secure applications without co-sponsoring a Formula 1 team? The modern threat landscape is a mess of AI-generated vulnerabilities, supply chain poisoning, and cloud misconfigurations. You don't need a seven-figure vendor budget to fight it.

In this 2-hour hands-on workshop, we will build a complete, automated AppSec pipeline using entirely open-source tools. We will wire up Opengrep for SAST, Trivy for containers, Checkov for infrastructure, and ZAP for DAST - piping the chaos into DefectDojo for centralized vulnerability management. We will also explore how to use local AI models to triage the inevitable mountain of false positives. You will walk away with a functional pipeline and a realistic understanding of where open-source excels, and where it falls apart.

SpeakerBio: Mackenzie

Mackenzie is a developer advocate with a passion for DevOps and code security. As the co-founder and former CTO of a health tech startup, he learnt first-hand how critical it is to build secure applications with robust developer operations.

Today as the Developer Advocate at GitGuardian, Mackenzie is able to share his passion for code security with developers and works closely with research teams to show how malicious actors discover and exploit vulnerabilities in code.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Social Engineering Community Village - Saturday - 16:30-17:59 PDT

Title: Cold Calls

Tags: Social Engineering Community Village | Creator Event/Activity

When: Saturday, Aug 8, 16:30 - 17:59 PDT

Where: LVCCW Level 3 W317-319 (Social Engineering Community Village) - [Map](#)

Description:

Ready for the hot seat? Step into the soundproof booth, grab a mystery target and three escalating objectives, and we'll place the call. Run by rekdt, Arty Boy, and Shadow Fox. First come, first served, so get your name on the Cold Call list!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Social Engineering Community Village - Sunday - 11:30-12:30 PDT

Title: Cold Calls

Tags: Social Engineering Community Village | Creator Event/Activity

When: Sunday, Aug 9, 11:30 - 12:30 PDT

Where: LVCCW Level 3 W317-319 (Social Engineering Community Village) - [Map](#)

Description:

Ready for the hot seat? Step into the soundproof booth, grab a mystery target and three escalating objectives, and we'll place the call. Run by rekdt, Arty Boy, and Shadow Fox. First come, first served, so get your name on the Cold Call list!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Social Engineering Community Village - Friday - 16:00-17:59 PDT

Title: Cold Calls

Tags: Social Engineering Community Village | Creator Event/Activity

When: Friday, Aug 7, 16:00 - 17:59 PDT

Where: LVCCW Level 3 W317-319 (Social Engineering Community Village) - [Map](#)

Description:

Ready for the hot seat? Step into the soundproof booth, grab a mystery target and three escalating objectives, and we'll place the call. Run by rekdt, Arty Boy, and Shadow Fox. First come, first served, so get your name on the Cold Call list!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Misc - Sunday - 10:00-10:59 PDT

Title: Coloring Reset

Tags: Women in Security and Privacy (WISP) | Creator Event/Activity

When: Sunday, Aug 9, 10:00 - 10:59 PDT

Where: LVCCW Level 1 Hall 4 1303 (Women in Security and Privacy (WISP) Community) - [Map](#)

Description:

Kick off your DEF CON morning with a creative reset. Color with WISP! Choose from different coloring pages and bring them to life with markers, crayons, and your own flair. Whether you're decompressing or collaborating on a shared poster, it's the perfect low-pressure space to connect, reflect, and color outside the lines.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Misc - Saturday - 10:00-10:59 PDT

Title: Coloring Reset

Tags: Women in Security and Privacy (WISP) | Creator Event/Activity

When: Saturday, Aug 8, 10:00 - 10:59 PDT

Where: LVCCW Level 1 Hall 4 1303 (Women in Security and Privacy (WISP) Community) - [Map](#)

Description:

Kick off your DEF CON morning with a creative reset. Color with WISP! Choose from different coloring pages and bring them to life with markers, crayons, and your own flair. Whether you're decompressing or collaborating on a shared poster, it's the perfect low-pressure space to connect, reflect, and color outside the lines.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Misc - Friday - 10:00-10:59 PDT

Title: Coloring Reset

Tags: Women in Security and Privacy (WISP) | Creator Event/Activity

When: Friday, Aug 7, 10:00 - 10:59 PDT

Where: LVCCW Level 1 Hall 4 1303 (Women in Security and Privacy (WISP) Community) - [Map](#)

Description:

Kick off your DEF CON morning with a creative reset. Color with WISP! Choose from different coloring pages and bring them to life with markers, crayons, and your own flair. Whether you're decompressing or collaborating on a shared poster, it's the perfect low-pressure space to connect, reflect, and color outside the lines.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: COM Hijacking Voodoo: Tradecraft, Detection Blind Spots, and the COM-Hunter

Tags: Red Team Village | Misc

When: Friday, Aug 7, 11:00 - 11:59 PDT

Where: LVCCW Level 1 Hall 1 309 (Red Team Village) Workshop Stage 2 - [Map](#)

Description:

Component Object Model (COM) is one of the most pervasive yet overlooked subsystems in Windows. Thousands of applications rely on COM objects for functionality, but the underlying registration mechanism creates opportunities for attackers to abuse the Windows registry to achieve stealthy persistence and code execution. Despite being used in real-world intrusions, COM hijacking remains under-documented and poorly understood by many defenders.

This talk explores the internals of COM registration and activation and demonstrates how attackers abuse registry-based class registrations, InprocServer32 entries, and per-user overrides to hijack legitimate COM objects. We will analyze common hijacking patterns, explain why many of them evade traditional detection logic, and highlight the operational advantages they offer during post-exploitation and persistence phases.

To help security professionals systematically identify these opportunities, this presentation introduces COM-Hunter, a research tool designed to enumerate and analyze hijackable COM objects across Windows systems. COM-Hunter maps CLSID registrations, identifies missing or user-overridable components, and highlights potential hijacking vectors that can be leveraged during red team engagements or security research.

Through practical demonstrations, we will show how COM-Hunter can be used to uncover previously overlooked hijack paths and how red teamers can turn these findings into reliable persistence mechanisms. The talk also discusses defensive considerations, including detection strategies, telemetry sources, and ways organizations can reduce the attack surface created by vulnerable COM registrations.

Attendees will leave with a deeper understanding of COM hijacking internals, practical offensive techniques, and a methodology for discovering new hijack opportunities in modern Windows environments.

SpeakerBio: Nikos "nickvourd" Vourdas, EY

Nikos Vourdas, also known as nickvourd or NCV, is a Senior Offensive Security Consultant based in the US. With over five years of professional experience, he has actively participated in various global Tiber-EU and iCAST Red Teaming engagements. Nikos has conducted full Red Teaming operations to major clients across retail, banking, shipping, construction industries. He holds OSCE3, OSCP, OSWP, CRTL, CRT0 and OASP certifications. Also, he has previously presented at DEF CON, DevSecCon, and various BSides events around the world. Nikos loves contributing to open-source projects and always starts his day at 05:00 AM with a refreshing jog while listening to French rap music.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Red Team Village - Saturday - 12:00-13:59 PDT

Title: Command & Conquer: Hands-on C2 Primer with Mythic

Tags: Red Team Village | Misc

When: Saturday, Aug 8, 12:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 1 309 (Red Team Village) Tactic Table 2 - [Map](#)

Description:

This hands-on workshop provides a unified view of C2 fundamentals for both offensive and defensive practitioners. Using the open-source Mythic framework, participants will deploy agents, handle callbacks, execute tasking with commentary on opsec and payload design considerations.

The session will also cover basic C2 infrastructure design including redirectors/domain fronting and an overview of Mythic feature sets. Students should leave armed with practical introductory experience operating Mythic for Red Team engagements.

The requested 2.5 hour timeslot should allow for at least two complete runs through the presentation and hands-on workshops as well as time for Q&A and subsequent "turnover" on the room for a new wave of attendees.

Participants must have the following equipment:

- A laptop capable of running Docker containers and/or macOS/Windows/Linux VMs. It is highly recommended that students do not use corporate assets for this workshop as they are likely to trigger AV/EDR when working with the example (default) payloads.
- If students wish to host Mythic themselves an x86 host/VM is required, however this will not be part of the workshop. We will provide a limited-access, cloud-hosted Mythic C2 server environment for students to connect to.

SpeakerBio: Logan MacLaren

Logan is the lead Offensive Security engineer at Huntress where he is responsible for planning and executing red team operations as well as bolstering incident response capability through purple team exercises. He has been a long time enthusiast in the security space, building a career spanning big data analytics, bug bounty, and offensive security.

Outside of his day job, Logan can often be found building and participating in CTF challenges, bug hunting in open source software, or learning new skills at conferences across the continent. He has had the honour of speaking at several DEFCON villages, NorthSec conferences, as well as multiple BSides and OWASP Ottawa events.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Commit, Push, Compromise: Attacking Modern GitHub Orgs

Tags: Red Team Village | Misc

When: Sunday, Aug 9, 11:00 - 11:59 PDT

Where: LVCCW Level 1 Hall 1 309 (Red Team Village) Workshop Stage 2 - [Map](#)

Description:

GitHub is where identity, automation, and production changes all meet, which makes it a great target. Once an attacker gets in, the distance between read access and shipping malicious code to production is often a lot shorter than teams expect.

This talk covers realistic attack paths into GitHub organizations. We start with initial access: device-code phishing and abuse of trusted GitHub Apps like the GitHub CLI. Then we follow the credentials, from long-lived Personal Access Tokens sitting on developer machines to short-lived secrets like GITHUB_TOKEN that leak through logs and artifacts, and show how both enable lateral movement and privilege escalation.

Then we get into a technique we call secret stomping. Anyone with write access to a repo can overwrite an Actions secret, including protected environment secrets reviewers assume are safe. Leak the real value first, then overwrite the secret with a payload that keeps the original value intact, and the pipeline stays green while your code runs on the runner. Using the org, repo, and environment scope hierarchy, you can shadow a secret in one repo without touching others, then delete it and leave nothing behind at the org level.

We close on the defensive side with detection strategies and response playbooks built around the signals that matter, plus how to get coverage into the places GitHub is hardest to watch. Blue teams leave with a checklist for locking down identities, tokens, integrations, and workflows. Red teams leave with a map of where GitHub controls break in practice.

After the talk we're running a hands-on workshop in a private GitHub org built for this, focused on secret stomping. You'll leak a secret, stomp it with a payload that keeps the pipeline green, and use scope shadowing to exploit your way onto a sensitive runner without tripping the obvious alarms. Bring a laptop.

Speakers: Andrew Buchanan, Max CM

SpeakerBio: Andrew Buchanan

Andrew Buchanan is a Senior Red Team Operator with over six years of offensive security experience spanning adversary simulation, penetration testing, and real-world attack execution.

Andrew has spent years conducting advanced red team engagements and security assessments across highly complex enterprise environments at one of Canada's largest financial institutions.

Andrew specializes in initial access and social engineering, having designed and delivered numerous campaigns that closely mirror real-world threat actor tradecraft. His work spans offensive operations across on-premises, cloud, and hybrid environments, with a particular focus on cloud attack surfaces, execution chains, and targeted phishing and pretexting campaigns.

SpeakerBio: Max CM

Max leads offensive security at Figment and brings over a decade of experience spanning national security, security research, and blockchain security. He has published multiple CVEs and conducts research focused on CI/CD pipeline security, threat modeling, secure key management, and practical security controls for high-risk systems.



Title: Compiling the World: A Binary Dataset Built from nixpkgs

Tags: Nix Vegas Community | Creator Talk/Panel

When: Saturday, Aug 8, 11:30 - 11:59 PDT

Where: LVCCW Level 1 Hall 3 1100 (Creator Stage 7) - [Map](#)

Description:

Reverse engineering binaries is slow, detailed work, but it's one of the few ways we have to verify what some software actually does. Machine learning might help improve some of those challenges, but only if you have high-quality, real-world ground truth to train and evaluate on. At MIT Lincoln Laboratory, we have built a large dataset for machine learning on x86_64 binaries using nixpkgs, taking advantage of Nix's reproducibility, package coverage, and instrumentable build environments. We compiled tens of thousands of C, C++, Rust, and Go packages, often multiple versions of each, with consistent compiler flags, captured source files, and debug information. From these, we extracted roughly 50 million functions and aligned with their source code and short descriptions. Possible applications include fine-tuning large language models for various binary tasks or training custom, highly efficient models for binary code understanding. I'll walk through what it takes to wrangle nixpkgs in an HPC environment at this scale and show how open build tooling like Nix can help us to better understand and analyze the software that we all depend on.

SpeakerBio: Chris Connelly, MIT Lincoln Laboratory

Chris Connelly is a Senior Technical Staff member at MIT Lincoln Laboratory in the Cyber Security and Information Sciences Division. Since joining the Laboratory in 2002, he has contributed to or led research, development, and evaluation programs in several areas, including malware analysis, vulnerability discovery, systems analysis, test automation technologies, large-scale distributed systems, and software architecture.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Composable Systems with NixOS MicroVMs

Tags: Nix Vegas Community | Creator Talk/Panel

When: Friday, Aug 7, 10:30 - 10:59 PDT

Where: LVCCW Level 1 Hall 4 1310 (Nix Vegas Community) - [Map](#)

Description:

MicroVMs make it easy to give every service, project, or person dedicated NixOS machines. We will use `microvm.nix` to build dev boxes, game servers, and sensitive services on hardware we control. Because each guest is simply a NixOS configuration, it can be reused, extended, rebuilt, and shared.

We will compare MicroVM isolation with other options, explain its limitations, and show how to compose useful machines from ordinary NixOS modules for yourself and those around you. We will finish with a look beyond a single host: how to preserve and back up these machines, then place them across hardware you own.

SpeakerBio: Alex Decious

I work on build systems and CI infrastructure for Shopify's monorepo using Nix, and run my own infrastructure as a systems lab for compute-heavy builds, distributed systems experiments, local LLMs, and hosting for myself and others.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Payment Village - Saturday - 16:00-16:45 PDT

Title: Compounding Interest: Exploiting the ATM Supply Chain

Tags: Payment Village | Creator Talk/Panel

When: Saturday, Aug 8, 16:00 - 16:45 PDT

Where: LVCCW Level 2 W204-205 (Payment Village) - [Map](#)

Description:

ATMs are the ultimate high-stakes target, often holding upwards of \$400,000 in a single enclosure. While the global financial industry relies on a narrow pool of manufacturers, the software supply chain securing these "vaults" remains an under-examined attack surface. Following my disclosure of 6 code execution vulnerabilities affecting Diebold Nixdorf at DEF CON 32, this research dives deeper into the foundational security layer: CryptoWare CryptoPro Secure Disk for BitLocker.

CryptoPro acts as a proprietary security wrapper, adding pre-boot authorization, custom TPM protections, and an obfuscated encryption layer to the standard BitLocker architecture. In this session, I will highlight the nuances of the CryptoPro architecture, including, secret storage through unallocated disk space, TPM sealing logic, and the layered crypto architecture used to secure system secrets. I will demonstrate how these deficiencies provide a path for code execution and full compromise of the Windows BitLocker encryption keys.

In addition to the technical walk through, I will release ragavan, a custom exploitation toolkit designed to automate secret extraction, decryption, TPM unsealing, and compromise of a CryptoPro-protected platform.

SpeakerBio: Matt Burch, Principal Security Researcher at Atredis Partners

Matt Burch is a Principal Security Researcher at Atredis Partners with 20 years of experience breaking things that aren't supposed to break. From the embedded components of ATM platforms to complex SCADA/OT environments, Matt specializes in identifying critical flaws in hardened, enterprise-class systems. He is best known for his research into ATM disk encryption and Mobile Device Management (MDM) security, some of which has been highlighted in Wired Magazine and presented at DEF CON 32.

Matt is a reverse engineer and tool developer who has authored and contributed to various public projects. His career spans roles as an offensive security lead, expert witness, and technical advisor. Matt's current research is a deep-dive into the ATM software supply chain, specifically targeting the subversion of TPM-backed roots of trust and the analysis of custom cryptographic primitives.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Compounding Interest: Exploiting the ATM Supply Chain

Tags: DEF CON Official Talk | Demo | Tool | Exploit

When: Saturday, Aug 8, 12:30 - 13:30 PDT

Where: LVCCW Level 1 Hall 3 904 (Main Track 4) - [Map](#)

Description:

ATMs are the ultimate high-stakes target, often holding upwards of \$400,000 in a single enclosure. While the global financial industry relies on a narrow pool of manufacturers, the software supply chain securing these "vaults" remains an underexamined attack surface. Following my disclosure of 6 code execution vulnerabilities affecting Diebold Nixdorf's Vynamic Security Suite (VSS) at DefCon32, this research dives deeper into the foundational security layer: CryptWare CryptoPro Secure Disk for BitLocker.

CryptoPro acts as a proprietary security wrapper, adding pre-boot authorization, custom TPM protections, and an obfuscated encryption layer to the standard BitLocker architecture. I will be disclosing 9 new CVEs that allow an unauthenticated adversary to dismantle the CryptoPro stack. Join me as I share my journey of locating secrets buried in unallocated disk space, abusing TPM sealing logic, and deconstruct CryptoPro's custom AES256 logic to recover the BitLocker keys. This presentation will highlight how a trusted security component became a critical backdoor.

In addition to the technical walk through, I will be releasing ragavan, a custom exploitation toolkit designed to automate secret extraction, decryption, TPM unsealing, and compromise of a CryptoPro-protected platform.

- Burch, Matt "Where's the Money: Defeating ATM Disk Encryption" DEFCON Media Server, <https://media.defcon.org/DEF%20CON%2032/DEF%20CON%2032%20presentations/DEF%20CON%2032%20-%20Matt%20Burch%20Where's%20the%20Money%20Defeating%20ATM%20Disk%20Encryption.pdf>
- Freingruber, R., and M. von Dach. "Manipulation of pre-boot authentication in CryptWare CryptoPro Secure Disk for BitLocker" SEC Consult, <https://sec-consult.com/vulnerability-lab/advisory/manipulation-of-pre-boot-authentication/>
- Diebold Nixdorf Legal Terms, <https://dnlegalterms.com/products/>
- Vynamic Security Suite 3.0 EULA, https://dnlegalterms.com/wp-content/uploads/2020/03/2020026_Diebold_Nixdorf_EULA_for_VYNAMIC_SECURITY_3.0.pdf
- Vynamic Security Suite 4.5 EULA, <https://dnlegalterms.com/wp-content/uploads/2024/10/Diebold-Nixdorf-Third-Party-EULA-for-Vynamic-Security-Suite-4.5.pdf>
- VirusTotal CryptoPro Client Installer, <https://www.virustotal.com/gui/file/235646487eed8cb648f9d05dafd3c25255b6c53a30aa87cae0ce061081d2b0b7>
- VirusTotal CryptoPro Server Installer, <https://www.virustotal.com/gui/file/1f42ac4f4d177dc2c38228e02d3c47ecfeb32ee7c17766b8e67145348274a8cc>
- cpsd it services GmbH. "CryptoPro Quick Install Guide", <https://secure-disk-for-bitlocker.com/quick-install-guide/>
- cpsd it services GmbH. "CryptoPro Secure Disk for BitLocker Administration Manual", <https://docslib.org/doc/7196170/cryptopro-secure-disk-for-bitlocker-administration-manual>
- Jean-Philippe Aumasson, "Serious Cryptography A practical Introduction to Modern Encryption" No Starch Press
- Christof Paar and Jan Pelzl, "Understanding Cryptography A Textbook for Students and Practitioners" Springer

SpeakerBio: Matt Burch, Principal Security Researcher at Atredis Partners

Matt Burch is a Principal Security Researcher at Atredis Partners with 20 years of experience breaking things that aren't supposed to break. From the embedded components of ATM platforms to complex SCADA/OT environments, Matt specializes in identifying critical flaws in hardened, enterprise-class systems. He is best known for his research into ATM disk encryption and Mobile Device Management (MDM) security, some of which has been highlighted in Wired Magazine and presented at DEF CON 32.

Matt is a reverse engineer and tool developer who has authored and contributed to various public projects. His career spans roles as an offensive security lead, expert witness, and technical advisor. Matt's current research is a deep-dive into the ATM

software supply chain, specifically targeting the subversion of TPM-backed roots of trust and the analysis of custom cryptographic primitives.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Condense Volumes, Connect Dots, Enrich Contexts: Scaling Root Cause Analysis and Automated Troubleshooting with ML

Tags: Middle Easterns & Africans in Cyber Security (MEACS) | Creator Talk/Panel

When: Saturday, Aug 8, 14:30 - 14:59 PDT

Where: LVCCW Level 1 Hall 3 1100 (Creator Stage 7) - [Map](#)

Description:

Learn to use ML to condense volumes by 80% without data loss by grouping related records and deduping their redundant field values. Learn how to use ML to auto-normalize records to a unified schema and enrich them with their most relevant tags and labels across objects, assets, entities, frameworks and controls. Use ML to correlate situationally relevant records, similar root causes and link causal sequences and behavior. Use AI to further troubleshoot, detect and remediate with rich-context.

SpeakerBio: Ezz Tahoun

Ezz Tahoun is an award-winning cybersecurity data scientist recognized globally for his innovations in applying AI to security operations.

He has keynoted, trained & presented at BlackHat US, Sector, MEA, Asia & EU, DEFCON, SANS Summits, all the top Bsides, Securityweek ICS Conference and GISEC among many others.

His groundbreaking work earned him a gold edison award and accolades from Yale, Princeton, Northwestern, NATO, Microsoft, and Canada's CSE.

At 19, Ezz began his PhD in Computer Sci at the Univ of Waterloo, quickly gaining recognition through over 20 influential papers and open-source tools.

His experience includes leading advanced AI security ops projects for Orange CyberDefense, Forescout, RBC, and Huawei US.

He holds certifications such as GIAC Advisory Board, aCCISO, CISM, CRISC, GCIH, CEH, PMP and GCP-Cloud Architect, and served as an adjunct professor in cyber defense and warfare.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Condense, Contextualize, and Correlate: Optimize Costs while Connecting the Dots at Scale

Tags: Middle Easterns & Africans in Cyber Security (MEACS) | Creator Talk/Panel

When: Friday, Aug 7, 17:00 - 17:30 PDT

Where: LVCCW Level 1 Hall 3 1100 (Creator Stage 7) - [Map](#)

Description:

Auto-condense telemetry volumes by 80% without data loss by grouping related records & deduping redundant values, with ML that auto-normalizes to a unified schema & auto-enriches data with relevant abstractive classifications, framework-aligned controls, contextual tags & environment labels. Use the efficiency with TKG ML to scale multi-level correlations & reveal all similarity & causality patterns & root causes. Use AI to automate troubleshooting, investigations, remediations & operations.

SpeakerBio: Ezz Tahoun

Ezz Tahoun is an award-winning cybersecurity data scientist recognized globally for his innovations in applying AI to security operations.

He has keynoted, trained & presented at BlackHat US, Sector, MEA, Asia & EU, DEFCON, SANS Summits, all the top Bsides, Securityweek ICS Conference and GISEC among many others.

His groundbreaking work earned him a gold edison award and accolades from Yale, Princeton, Northwestern, NATO, Microsoft, and Canada's CSE.

At 19, Ezz began his PhD in Computer Sci at the Univ of Waterloo, quickly gaining recognition through over 20 influential papers and open-source tools.

His experience includes leading advanced AI security ops projects for Orange CyberDefense, Forescout, RBC, and Huawei US.

He holds certifications such as GIAC Advisory Board, aCCISO, CISM, CRISC, GCIH, CEH, PMP and GCP-Cloud Architect, and served as an adjunct professor in cyber defense and warfare.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Social Gatherings/Events - Thursday - 21:00-23:59 PDT

Title: Conference Planners Meetup

Tags: Meetup

When: Thursday, Aug 6, 21:00 - 23:59 PDT

Where: LVCCW Level 2 W212 (Misc Meeting Room) - [Map](#)

Description:

Are you a conference planner, manager, technologist, etc.? Feel like chatting about what we do, trading contact info, or just grabbing a few drinks with colleagues? This will be a meetup for those of us involved in conference planning and management. There won't be any kind of schedule or agenda. Informal conversation is the name of the game.

At least one person from the Hacker Tracker (and ConfMgr) team will be here. You're welcome to ask questions, leave feedback (good or bad), ask for help with some problem you're having, etc.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Blacks In Cyber Village - Friday - 15:30-15:55 PDT

Title: Configuring Your Favorite Platforms to Prioritize DNS

Tags: Blacks In Cyber Village | Creator Talk/Panel

When: Friday, Aug 7, 15:30 - 15:55 PDT

Where: LVCCW Level 3 W322-W324 (BIC Village) - [Map](#)

Description:

Explore how to leverage infrastructure OSINT data, such as passive DNS and domain registration records, to enhance your threat intelligence and protect your organization without exhausting budgets. In this demo, DomainTools Senior Security Advisor Malachi Walker will discuss how security teams can develop advanced techniques for continuous and explainable intelligence. Then, DomainTools Principal Product Manager Anthony Johnson will demonstrate how these concepts can be applied to build AI-driven product layers that draw domain intelligence from standard LLMs like ChatGPT, Claude, Gemini, and Copilot. Discover innovations that reduce triage time, improve early warnings, and automate campaign linkages, transforming your existing intelligence practices.

Speakers: Malachi Walker, Anthony Johnson

SpeakerBio: Malachi Walker, DomainTools

Malachi Walker, DomainTools Senior Security Advisor, brings extensive experience in information security, spanning DNS, cyberspace crime and conflict, and cybersecurity governance and program design. They have previously worked in FTI Consulting's Cybersecurity practice and led product and brand protection efforts at WhiteHawk Inc. Malachi holds a Master's in Business Administration with a concentration in Cybersecurity Management from Virginia Polytechnic Institute and State University.

SpeakerBio: Anthony Johnson, DomainTools

Anthony Johnson, DomainTools Principal Product Manager, has nearly 15 years of experience in cybersecurity. His background includes forensics, analytics, and product management, gained through work with the US Military, Casino Gaming, and other security-focused organizations.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Connectivity as Control in the European High North

Tags: Policy @ DEF CON | Creator Talk/Panel

When: Friday, Aug 7, 13:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 3 801 (Creator Stage 1) - [Map](#)

Description:

Between 2022 and 2024, the European High North saw three events at three attribution confidence levels. One segment of Svalbard's twin fibre system failed—Norwegian police closed the case with no state-actor finding. AcidRain wiped tens of thousands of Viasat SurfBeam2 modems via a ground-segment management-plane compromise—attributed to GRU by US/UK/EU in May 2022. GNSS interference over eastern Finnmark persisted 2019–2024—assessed by Norwegian services as Russian EW largely spilling from Kola. Three attributions. Three regimes. No mechanism that treats them as one. UNCLOS cable protection varies by zone (Art 79 shelf; Art 113 high seas; Art 58 EEZ). The 1884 Cables Convention—still in force—governs outside territorial waters. Svalbard Treaty reach into the FPZ is contested. NATO's cumulative-effects language has no classification framework. The 2023–24 Baltic sequence (Balticconnector; C-Lion1/BCS; Estlink-2/Eagle S) is the same play in the active theatre NATO CUI Cell, Baltic Sentry, EU CER/NIS2, JEF and NORDEFCO already cover — and still falls through. We propose an allies-first application of UNDRR Hazard Information Profiles to adversarial compound operations: indicators, authorities, a 2027 milestone. Classification stops no cable. A common record is the precondition for everything that will.

Speakers: Szymon Skalski, Patricia Vargas Leon, Jorge Acevedo Canabal

SpeakerBio: Szymon Skalski, Jagiellonian University PL

Szymon is a PhD Candidate in the School of Social Sciences at Jagiellonian University and a Senior Expert and NASK National Research Institute in Poland. He is also affiliated with the Ostrom Workshop at Indiana University, where he leads the working group on Environmental Security and Technological Risk in Conflict. He has served on cybersecurity expert panels at the Polish Ministry of Digital Affairs and the Polish Bank Association. He is also a fellow of the European Law Institute, member of FIDMA and Virtual Routes European PhD Cybersecurity Accelerator Programme. For the past three years, he has participated in NATO's Locked Shields exercises, representing Poland for two years and, in 2026, organizing the exercises on behalf of the CCDCOE in the legal domain. He is a researcher and scholarship holder of grants from the National Science Centre in Poland in the fields of insurance and digital security. He publishes in international academic journals in the fields of cybersecurity, insurance, tort law, and international law.

SpeakerBio: Patricia Vargas Leon, Ostrom Workshop Indiana University US, Yale Law School

Patricia A. Vargas León is a Visiting Fellow at Yale Law School's Information Society Project, a Cybersecurity Research Postdoctoral Fellow at Indiana University's Ostrom Workshop, and a Visiting Scholar in Internet Governance at the Catholic University of Uruguay. Her research bridges law, policy, and technology — focusing on Internet governance, cybersecurity, international law, and the law of the sea. She is particularly interested in how governments control Internet infrastructure, network neutrality, and regulatory parallels between the law of the sea and cyberspace. Her doctoral dissertation examines Internet blackouts across political regimes and how states restrict digital connectivity. Before academia, Patricia practiced law in the private sector for nearly a decade and brings over two decades of international law experience to her work, including a consultancy with the UN Division for Ocean Affairs and the Law of the Sea (DOALOS). She also served as a Google Policy Fellow during her doctoral studies. Patricia holds a Ph.D. and M.S. in Information Science and Technology from Syracuse University and a law degree from the Pontifical Catholic University of Peru. Her dual training positions her to address complex questions at the intersection of technology, governance, and international law.

SpeakerBio: Jorge Acevedo Canabal, Ostrom Workshop Indiana University US

Jorge Acevedo Canabal, MD (University of Puerto Rico School of Medicine, Magna Cum Laude), is a physician and Visiting Scholar at the Ostrom Workshop, Indiana University, working on research that sits at the intersection of healthcare, public health, and cybersecurity, applying epidemiological and disaster medicine methods to map patient harm attributable to healthcare cyberattacks and technological hazards. He previously served as Chief Medical Officer of the Puerto Rico Science, Technology and Research Trust, and currently serves as advisor to the Biohacking Village and Raíces Cyber Org.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Container Escapes 101

Tags: Intermediate | AppSec Village | Creator Workshop

When: Friday, Aug 7, 14:30 - 16:59 PDT

Where: LVCCW Level 1 Hall 2 604 (Appsec Village) Classroom - [Map](#)

Description:

Containers aren't tiny fortresses. They're leaky rowboats unless you know what you're doing. This hands-on workshop demystifies container security layer by layer, showing how real-world missteps in runtime, image, and host configurations open doors to escapes, persistence, and lateral movement. We'll dissect how containers actually work, walk through common isolation failures, and demonstrate how attackers exploit weak assumptions. Whether you're building, securing, or regulating containerized apps, you'll leave with a threat model, practical tools, and maybe a new trick or two for *literally* popping out of the box.

SpeakerBio: some-natalie

Natalie is a principal solutions engineer at XBOW serving the public sector market. She spent years designing, building, and leading complex systems in regulated environments at a major systems integrator, but has also taken her career in many other directions - including detours into project management, systems engineering, and teaching.

She's passionate about diversity in technology and empowering engineers to build better.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Container Escapes Are Not Magic. Here Is How They Actually Work.

Tags: AppSec Village | Creator Talk/Panel | All Audiences

When: Friday, Aug 7, 12:30 - 12:59 PDT

Where: LVCCW Level 1 Hall 2 604 (Appsec Village) Main Stage - [Map](#)

Description:

Container escapes sound scary and complicated. In practice, most of them come down to a handful of misconfigurations that show up in production environments all the time. Overprivileged containers, exposed Docker sockets, weak seccomp profiles, and poorly scoped capabilities. This talk demystifies container escapes for AppSec practitioners. We will walk through three real escape techniques live inside Docker environments running on Google Cloud, explain exactly why each one works, and then show the configuration changes and detection controls that prevent them. No black magic. Just misconfigurations you can find and fix right now, in environments that look a lot like yours.

SpeakerBio: Advait Patel

Advait Patel is a Senior Site Reliability Engineer at Broadcom and the creator of DockSec, an open-source, AI-powered Docker security analyzer.

Advait is a Docker Captain, Google Developer Expert and regular speaker at major security and developer conferences, including QConAI Boston, SANS CloudSecNext, OWASP GlobalAppSec US, OWASP SnowFROC, PlatformCon, Linux Security Summit North America, O'Reilly Media AI CodeCon, Redgate Cloud Summit, CornCon, ISACA, Silicon Valley Cybersecurity Conference.

His work sits at the intersection of AI, security, and developer workflows, with a particular focus on how emerging technologies like LLMs are reshaping modern development, CI/CD pipelines, and Git-based collaboration. As part of the Git and DevOps community, he advocates for secure-by-default design, developer empowerment, and open-source tooling that puts security in the hands of those who build the future.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Contests - Sunday - 10:00-10:30 PDT

Title: Contest Awards

Tags: Social Engineering Community Village | Contest

When: Sunday, Aug 9, 10:00 - 10:30 PDT

Where: LVCCW Level 3 W317-319 (Social Engineering Community Village) - [Map](#)

Description:

See who won in our village! During this time we'll present the SECVV and BOTB winners, as well as the much-coveted Dundies!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

DEF CON Talks - Sunday - 13:30-14:59 PDT

Title: Contest Closing Ceremonies & Awards

Tags: DEF CON Official Talk

When: Sunday, Aug 9, 13:30 - 14:59 PDT

Where: LVCCW Level 1 Hall 3 1006,904 (Main Tracks 1,4) - [Map](#)

Description:



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Control + C = Control Me

Tags: Red Team Village | Misc

When: Saturday, Aug 8, 16:00 - 16:59 PDT

Where: LVCCW Level 1 Hall 1 309 (Red Team Village) Workshop Stage 1 - [Map](#)

Description:

Demos (Desktop Only at the moment): <https://doctoreww.github.io/EvilFontTool/>

Tool: <https://github.com/DoctorEww/EvilFontTool>

General: Workshop goes into evil fonts and how to use them in a red team to get free shells, also hints at a tool to make it easier (saving most of the tool stuff for the tactic)

Tactic will go into using the tool to create malicious word docs for social engineering / popping a shell.

Description: For decades, cybersecurity has taught us to validate what we click, what we download, and what we run. Analysts learn to inspect URLs carefully, read every line, and challenge every prompt or popup that doesn't look quite right. But in all this vigilance, we've ignored a foundational assumption. We trust our eyes. We trust that what we see is what the system sees. This talk demonstrates why that assumption puts us at risk.

In the modern computing stack, very little sits closer to human perception than fonts. They are in browsers, PDFs, document editors, terminals, IDEs, chat apps, and nearly every interface in between. Yet despite their ubiquity, fonts are almost never treated as part of the security boundary. They're handled as passive design elements, harmless vessels used solely to shape text. Users trust them implicitly. This session introduces a new class of "evil font" attacks. With evil font attacks, red teamers can create situations where a user believes they are copying, clicking, or executing one thing... while the machine processes something entirely different.

Evil font attacks don't depend on JavaScript, macros, or browser exploits. Evil fonts work because there is no reason that a specific letter needs to look the way it does. In other words, the letter "A" only looks like an "A" because that's how my font drew it. With clever font manipulation a red teamer can make the letter "A" look like any other letter. For example, while a user might see the letter "B" the computer would still see the letter "A" represented by the underlying ASCII hex value. By manipulating fonts, files no longer have a single meaning... They mean one thing to a human reader, and another thing to a computer.

Once you realize this trust boundary is broken, there are so many ways to abuse this.

During the session, we walk through three attack scenarios usable by red teams; each scenario highlights a different security boundary where fonts exert control.

Clipboard deception in modern browsers Clipboard attacks typically require JavaScript, event hijacking, or social engineering. With evil fonts you can poison a clipboard on webpages without any JavaScript. With evil fonts an attacker can make on-screen text appear safe (e.g., "echo hello world" or "https://google.com") while the underlying copied text is entirely different. Users believe they are copying the text they verified with their eyes, but instead the clipboard receives text the attacker controls.

Document poisoning: Like browsers, documents like docx and pdf files can be poisoned by evil fonts. In this portion of the talk, we explore how to poison word and pdf files with malicious links and commands. These documents can be emailed for deception based social engineering. More insidious, evil fonts can be used to poison existing documents within a target such as how to's and infrastructure guides. By poisoning documents, red teamers can turn simple shared drive access into credentials and shells.

AI era submission manipulation: The rise of AI powered document processing introduces a new frontier for deception. Modern systems summarize text, extract entities, detect sentiment, identify anomalies, and evaluate authenticity. Evil fonts can exploit this by making the text look safe to the computer... but when read by a user, it displays malicious content. This manipulation can skew automated summaries, risk scoring, keyword extraction, plagiarism detection, and content filtering.

Please let me know if you have any questions! Thanks, Andrew

SpeakerBio: Andrew Griess

Andrew Griess is a Red Teamer at Centene who gets paid to break things and calls it a career. With 3 years of professional red team experience, he's made it their mission to think like an attacker while not succumbing to the dark side. When not poking holes in things for money, Andrew is deep in security research — chasing the next interesting bug, developing new techniques or going down rabbit holes that started as "just a quick look."



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Counting the Dead in the Digital Siege: Detection Infrastructure for Cyber-Mapping Patient Harm

Tags: Biohacking Village | Creator Talk/Panel

When: Friday, Aug 7, 10:00 - 10:45 PDT

Where: LVCCW Level 1 Hall 3 1105 (Creator Stage 3) - [Map](#)

Description:

Ransomware Kills Patients. We Can't Prove It. Here's How We Fix That.

Ransomware attacks on hospitals kill people. That's not a hypothesis — it's in the data. A peer-reviewed analysis of Medicare claims (American Economic Journal: Economic Policy, 2026) puts in-hospital mortality at 34 to 38 percent higher during attacks. The dead are disproportionately elderly, critically ill, and patients of color. Dameff et al. (2023) documented emergency department spillover. Neprash, Dameff, and Tully (2024) traced the same pattern through the Change Healthcare attack.

The mechanism isn't exotic. Encrypted EHRs mean clinicians are flying blind — no medication history, no imaging, no labs. Networked infusion pumps, ventilators, and monitors drop to manual. Ambulances get diverted, stacking patients at facilities that weren't hit. In rural areas, transfer times go from nine minutes to thirty-three. Here's the deeper problem: these deaths are architecturally invisible.

No ICD code exists for "died because the hospital's network was encrypted." No death certificate asks whether the hospital was under cyberattack. No public health surveillance system captures excess mortality from clinical failure caused by ransomware. Mandatory reporting requirements attach to data breach — not patient harm. Voluntary harm-reporting channels exist, but they're anonymous and sporadic. The visible signal is a fraction of what's actually happening.

This isn't a technical gap. It's a design failure in the detection infrastructure itself.

This talk makes the case for cyber-harm epidemiology. Using a forthcoming law review article, we show that existing systems — ICD external-cause coding, NCHS disaster-death certification, SNOMED CT alignment, the Sendai Framework's Hazard Information Profiles (2025) and Global Disaster-Related Statistics Framework (2026) — can be adapted right now to make cyber-attributable patient deaths visible at population scale. No new treaties required.

Better detection produces better attribution. Better attribution makes state obligations under the right to life and the protection of medical units enforceable — not aspirational.

The deaths are real. The tools to count them exist. We just haven't connected them yet. That's what this talk is about.

Speakers: Jorge Acevedo Canabal, Scott Shackelford, Szymon Skalski

SpeakerBio: Jorge Acevedo Canabal, Ostrom Workshop Indiana University US

Jorge Acevedo Canabal, MD (University of Puerto Rico School of Medicine, Magna Cum Laude), is a physician and Visiting Scholar at the Ostrom Workshop, Indiana University, working on research that sits at the intersection of healthcare, public health, and cybersecurity, applying epidemiological and disaster medicine methods to map patient harm attributable to healthcare cyberattacks and technological hazards. He previously served as Chief Medical Officer of the Puerto Rico Science, Technology and Research Trust, and currently serves as advisor to the Biohacking Village and Raíces Cyber Org.

SpeakerBio: Scott Shackelford

Scott J. Shackelford is Associate Vice President and Vice Chancellor for Research at Indiana University Bloomington and

Provost Professor of Business Law & Ethics at the IU Kelley School of Business. He serves as Executive Director of both the Ostrom Workshop and the Center for Applied Cybersecurity Research, and directs the Ostrom Workshop Program on Cybersecurity & Internet Governance. He is also an Affiliated Scholar at Harvard Kennedy School's Belfer Center and Stanford's Center for Internet and Society. Scott has authored over 100 articles, book chapters, and essays, with research featured in Politico, NPR, CNN, Forbes, Time, and the Washington Post. His books include *The Internet of Things: What Everyone Needs to Know* (2020) and *Managing Cyber Attacks in International Law, Business, and Relations* (2014). His honors include a Harvard Research Fellowship, a Stanford Hoover National Fellowship, the 2015 Elinor Ostrom Award, and the 2022 Poets & Quants Best 40-Under-40 MBA Professors Award.

SpeakerBio: Szymon Skalski, Jagiellonian University PL

Szymon is a PhD Candidate in the School of Social Sciences at Jagiellonian University and a Senior Expert and NASK National Research Institute in Poland. He is also affiliated with the Ostrom Workshop at Indiana University, where he leads the working group on Environmental Security and Technological Risk in Conflict. He has served on cybersecurity expert panels at the Polish Ministry of Digital Affairs and the Polish Bank Association. He is also a fellow of the European Law Institute, member of FIDMA and Virtual Routes European PhD Cybersecurity Accelerator Programme. For the past three years, he has participated in NATO's Locked Shields exercises, representing Poland for two years and, in 2026, organizing the exercises on behalf of the CCDCOE in the legal domain. He is a researcher and scholarship holder of grants from the National Science Centre in Poland in the fields of insurance and digital security. He publishes in international academic journals in the fields of cybersecurity, insurance, tort law, and international law.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Cove: Compositional and Verifiable Confidential Computing Workflows

Tags: Crypto & Privacy Village | Creator Talk/Panel

When: Sunday, Aug 9, 11:00 - 11:30 PDT

Where: LVCCW Level 1 Hall 3 1102 (Creator Stage 6) - [Map](#)

Description:

Confidential computing systems involve computation over private inputs held by mutually distrusting parties while producing public, cryptographically verifiable evidence of what was computed. Trusted execution environments (TEEs) are a practical building block for these systems, enabling code to run inside hardware-encrypted enclaves that emit attestations binding a measurement of the loaded code to genuine hardware. We present Cove, a framework that composes attested computations into multi-stage, multi-party workflows structured as directed acyclic graphs. Each node runs in its own enclave, decrypts private inputs only under attestation-gated key release, and emits a certificate that downstream nodes can require as a cryptographic precondition before consuming upstream artifacts; anyone holding the workflow bytes and the TEE vendor's attestation roots can verify the whole chain non-interactively. We show that a small set of reusable primitives - confidential artifact provisioning, encrypted dynamic outputs, attested ephemeral-key channels (RA-TLS), and certificate-gated preconditions - compose into systems that lift attestation from verified code identity to verified runtime properties, and use this to express practical applications in secure AI systems including confidential AI inference, attested AI benchmarks, and training-code verification. We give an open-source reference implementation on Intel TDX via Phala Cloud's dstack and demonstrate end-to-end feasibility with an attested benchmark workflow.

Speakers: Stephanie, Robin, Erika Lee

SpeakerBio: Stephanie

Stephanie is a research engineer working on AI security and safety. Her research interests include adversarial robustness, agent security and verifiable AI deployments. Previously, she was at Meta, where she worked on AI safety and security evaluations (CyberSecEval) and guardrails (PromptGuard, LlamaFirewall), and prior to that she worked on application security for web and mobile.

SpeakerBio: Robin

Robin is a Member of Technical Staff at Inferact (maintainer of vLLM), working towards the best inference stack of the future. Previously he worked as a software engineer at Near Protocol, Meta, Google, and Twitter. His interests include application security, model red-teaming, distributed systems, and GPU performance optimization.

SpeakerBio: Erika Lee

Erika Lee is a 3rd-year Math-Computer Science undergraduate student at UC San Diego and a MATS 9.1 AI Security Fellow. Her research interests are in verifiable and privacy-preserving AI, and building secure and trustworthy AI systems. She previously interned with the US Department of Defense's AI/ML portfolio and the U.S. Army, working on deploying AI/ML systems in classified environments.

Bing-Jyue Chen is a 3rd-year PhD candidate in Computer Science at UIUC. His current research focuses on zero knowledge machine learning (zkml). He is also interested in verifiable AI, privacy-preserving machine learning, and advanced cryptography.

Daniel Kang is an assistant professor at UIUC in the computer science department. His research focuses on making analytics with machine learning easy for scientists and analysts to use, and has been supported by Google, the Open Philanthropy project, Emergent Ventures, and others. He has consulted at OpenAI, Google, Microsoft, hedge funds, and other companies to

support their ML deployments, and advised a number of startups.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Quantum Village - Friday - 16:30-16:59 PDT

Title: Covert Quantum Computing - a new quantum security paradigm

Tags: Quantum Village | Creator Talk/Panel

When: Friday, Aug 7, 16:30 - 16:59 PDT

Where: LVCCW Level 1 Hall 3 1104 (Creator Stage 4) - [Map](#)

Description:

Quantum computers will inevitably move to multi-tenant systems for efficiency and throughput, with many users sharing a single QPU. This talk will discuss the realities of threats facing quantum computing 'as a service' and what is particularly specific to quantum computing. We'll get you started on understanding the quantum computing tech stack, and work through a few examples of possible attacks and mitigation techniques, wrapping up our newly developed security paradigm of covert quantum computing. All of the examples presented in this talk can be run by anyone with an internet connection and an email address. This talk is for anyone curious about attacks (and mitigation) techniques in quantum computing, and similarly how to build and test new ideas. A quantum background is not required!

SpeakerBio: Evan Anderson, UMD

Evan is a postdoctoral researcher at the University of Maryland focusing on photonic (and atomic) quantum computing architectures.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Contests - Sunday - 10:00-11:59 PDT

Title: Crack Me If You Can 2026

Tags: Crack Me If You Can 2026 | Contest

When: Sunday, Aug 9, 10:00 - 11:59 PDT

Where: LVCCW Level 1 Hall 1 106 (Crack me if you can) - [Map](#)

Description:

Time is of the essence! You will have 48 hours to crack as many hashes and files as possible.

Pamama, a US-based data broker had a massive data breach. Profiles on over a billion people, containing all the information amassed about them. It is alleged that the company siphoned records from different government agencies around the world, as well. The dump was encrypted, and regulators are downplaying the breach claiming no damage was done. A bill has been fast-tracked in Congress to exempt Pamama from any investigations, including illegally shield them from GDPR violations. This led to accusations that Pamama has bought or blackmailed members of congress.

Crack the staff's accounts and encrypted files to demonstrate the extent of the exposure and the need for individuals to get restitution and compensation, and to find smoking gun evidence of collusion so that the corruption can be fully exposed before the legislation goes forward.

Participant Prerequisites

Open to all, but pre-registration is recommended. Compete in the Street class for individuals or small teams, or in Pro if you do not want to sleep all weekend. Check out past years' contests at <https://contest.korelogic.com/> , or the Password Village site for an introduction to password cracking and links to other resources: <https://passwordvillage.org/>

Pre-Qualifications

None.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Contests - Saturday - 10:00-17:59 PDT

Title: Crack Me If You Can 2026

Tags: Crack Me If You Can 2026 | Contest

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 106 (Crack me if you can) - [Map](#)

Description:

Time is of the essence! You will have 48 hours to crack as many hashes and files as possible.

Pamama, a US-based data broker had a massive data breach. Profiles on over a billion people, containing all the information amassed about them. It is alleged that the company siphoned records from different government agencies around the world, as well. The dump was encrypted, and regulators are downplaying the breach claiming no damage was done. A bill has been fast-tracked in Congress to exempt Pamama from any investigations, including illegally shield them from GDPR violations. This led to accusations that Pamama has bought or blackmailed members of congress.

Crack the staff's accounts and encrypted files to demonstrate the extent of the exposure and the need for individuals to get restitution and compensation, and to find smoking gun evidence of collusion so that the corruption can be fully exposed before the legislation goes forward.

Participant Prerequisites

Open to all, but pre-registration is recommended. Compete in the Street class for individuals or small teams, or in Pro if you do not want to sleep all weekend. Check out past years' contests at <https://contest.korelogic.com/> , or the Password Village site for an introduction to password cracking and links to other resources: <https://passwordvillage.org/>

Pre-Qualifications

None.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Contests - Friday - 10:00-17:59 PDT

Title: Crack Me If You Can 2026

Tags: Crack Me If You Can 2026 | Contest

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 106 (Crack me if you can) - [Map](#)

Description:

Time is of the essence! You will have 48 hours to crack as many hashes and files as possible.

Pamama, a US-based data broker had a massive data breach. Profiles on over a billion people, containing all the information amassed about them. It is alleged that the company siphoned records from different government agencies around the world, as well. The dump was encrypted, and regulators are downplaying the breach claiming no damage was done. A bill has been fast-tracked in Congress to exempt Pamama from any investigations, including illegally shield them from GDPR violations. This led to accusations that Pamama has bought or blackmailed members of congress.

Crack the staff's accounts and encrypted files to demonstrate the extent of the exposure and the need for individuals to get restitution and compensation, and to find smoking gun evidence of collusion so that the corruption can be fully exposed before the legislation goes forward.

Participant Prerequisites

Open to all, but pre-registration is recommended. Compete in the Street class for individuals or small teams, or in Pro if you do not want to sleep all weekend. Check out past years' contests at <https://contest.korelogic.com/> , or the Password Village site for an introduction to password cracking and links to other resources: <https://passwordvillage.org/>

Pre-Qualifications

None.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Contests - Sunday - 10:00-11:59 PDT

Title: Crack the Core

Tags: Crack the Core | Contest

When: Sunday, Aug 9, 10:00 - 11:59 PDT

Where: LVCCW Level 1 Hall 1 214 (Crack the Core) - [Map](#)

Description:

Welcome to Crack the Core—a true test of lockpicking skills. Competitors will work through a variety of locks ranging in different difficulties, technologies, and configurations. From standard off-the-shelf locks to evil creations from the community. Locks will be presented in a variety of ways, ranging from your traditional deadbolt to much, much more. Just wait until you see what we have in store for you...

Challenges will not only test traditional lockpicking skills but force competitors to interact with different “environments,” work through various challenges, and adapt to what's presented. Collect the most points, you go home the winner—it's that simple...

Bring your tools. Bring your focus. The locks will be waiting.

Participant Prerequisites

Basic tools will be available for use but it is highly recommended to bring your own tools. This may include lockpicks, bypass tools, vices, etc. Destructive entry is not allowed and associated tools will not be needed.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Contests - Saturday - 10:00-17:59 PDT

Title: Crack the Core

Tags: Crack the Core | Contest

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 214 (Crack the Core) - [Map](#)

Description:

Welcome to Crack the Core—a true test of lockpicking skills. Competitors will work through a variety of locks ranging in different difficulties, technologies, and configurations. From standard off-the-shelf locks to evil creations from the community. Locks will be presented in a variety of ways, ranging from your traditional deadbolt to much, much more. Just wait until you see what we have in store for you...

Challenges will not only test traditional lockpicking skills but force competitors to interact with different “environments,” work through various challenges, and adapt to what's presented. Collect the most points, you go home the winner—it's that simple...

Bring your tools. Bring your focus. The locks will be waiting.

Participant Prerequisites

Basic tools will be available for use but it is highly recommended to bring your own tools. This may include lockpicks, bypass tools, vices, etc. Destructive entry is not allowed and associated tools will not be needed.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Contests - Friday - 10:00-17:59 PDT

Title: Crack the Core

Tags: Crack the Core | Contest

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 214 (Crack the Core) - [Map](#)

Description:

Welcome to Crack the Core—a true test of lockpicking skills. Competitors will work through a variety of locks ranging in different difficulties, technologies, and configurations. From standard off-the-shelf locks to evil creations from the community. Locks will be presented in a variety of ways, ranging from your traditional deadbolt to much, much more. Just wait until you see what we have in store for you...

Challenges will not only test traditional lockpicking skills but force competitors to interact with different “environments,” work through various challenges, and adapt to what's presented. Collect the most points, you go home the winner—it's that simple...

Bring your tools. Bring your focus. The locks will be waiting.

Participant Prerequisites

Basic tools will be available for use but it is highly recommended to bring your own tools. This may include lockpicks, bypass tools, vices, etc. Destructive entry is not allowed and associated tools will not be needed.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Cracking North Korea's Information Control: How Smugglers, Defectors, and Technologists are Breaking Open the World's Most Locked-Down Information System

Tags: DEF CON Official Talk | Demo

When: Saturday, Aug 8, 14:00 - 14:59 PDT

Where: LVCCW Level 1 Hall 3 903 (Main Track 5) - [Map](#)

Description:

North Korea operates the world's most extreme digital environment. Its custom Android OS enforces an "allowlist" ecosystem where media and apps require state-issued cryptographic signatures to run, while background daemons capture secret screenshots to log "illegal" activity. In this restrictive environment, the stakes for accessing outside information are measured in prison sentences and public executions.

Yet, the hackers are active. This talk deconstructs the regime's information control systems—from signature-verification logic to TraceViewer forensics—and reveals how a network of defectors and technologists is fighting back. We will demo Pigeon, a working SELFSIGN spoof that bypasses handset verification, and discuss eMMC chip-off techniques used to study device internals, and look at Windows data concealment methods used by defectors.

This isn't just a technology briefing; it's an offensive security call for support. I will map out a unique and intriguing engineering backlog which includes media obfuscation tools, Android internals research, binary analysis, anti-forensics, and hardware hacking. I will show how these skills directly translate into freedom-of-information tool development. Built and validated through iterative testing with defectors, some of these technologies are operational already today.

- Korean Ministry of Unification: Annual North Korean Refugee Arrival Statistics: https://www.unikorea.go.kr/eng_unikorea/
- Citizen Lab: Red Star OS Analysis (2015): <https://citizenlab.ca/2015/09/red-star-os/>
- 38 North: North Korean technology reporting: <https://www.38north.org>
- Martyn Williams: North Korea Tech: <https://www.northkoreatech.org>
- Defector interviews and memoirs
- Jieun Baek: North Korea's Hidden Revolution

SpeakerBio: JDT, Liberty in North Korea

JDT brings over a decade of cybersecurity expertise to his role as Chief Technology Officer at LiNK. Before joining the organization, he served as the lead specialist for the U.S. Department of Homeland Security's HQ Threat Hunt team, following ten years spent in incident response and red-teaming across the banking, retail, and tech sectors.

After volunteering for the North Korean human rights movement in 2019, JDT stepped into the CTO role in 2025 to spearhead the development of tools designed to pierce the world's most restrictive information environment. By repurposing his deep understanding of adversary tradecraft, he develops unconventional technologies that empower North Koreans to access outside information safely and bypass state surveillance.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Cracking the Cybersecurity Career Code with the Cyber Color Wheel

Tags: .EDU Community | Creator Talk/Panel

When: Friday, Aug 7, 11:00 - 11:59 PDT

Where: LVCCW Level 1 Hall 4 1418 (.EDU Community) - [Map](#)

Description:

Giveaway: Two raffles for one copy of:

See Yourself in Cyber: Security Careers Beyond Hacking

SpeakerBio: Shavvon "TheSiren" Cintron

Shavvon Cintron spent the last decade climbing the IT ladder, now working in IT and cybersecurity within the healthcare space. She's got an MS in Cybersecurity from Pace, a BS in Criminal Justice from CUNY John Jay, and a 2025 SANS Institute Difference Makers Rising Star nod, so somebody thinks she's doing something right. When she's not at her day job, she's Director of Women's Education for the Women's Society of Cyberjutsu, building the programs she wishes existed when she was trying to break in. She goes by "Siren of the Cyber Sea." Get too close and you might not want to leave.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Cracking ValleyRAT: From Builder Secrets to Kernel Rootkits

Tags: Malware Village | Creator Talk/Panel

When: Saturday, Aug 8, 10:00 - 10:35 PDT

Where: LVCCW Level 1 Hall 2 600 (Malware Village) Talks - [Map](#)

Description:

Abstract:

What happens when a leaked malware builder suddenly opens the door for anyone — from low-tier criminals to advanced operators — to deploy a backdoor armed with a kernel-capable rootkit? What happens when that rootkit still carries valid signatures, and Windows 11 willingly loads it?

In this talk, Check Point Research unveils a comprehensive reverse engineering of ValleyRAT, a modular backdoor family also known as Winos/Winos4.0. By dissecting the publicly leaked builder and its development artifacts, we reconstruct the malware's architecture from the ground up, uncovering a highly organized plugin ecosystem and coding style that reveals a small, specialized team with deep knowledge of the Windows kernel.

The standout finding: ValleyRAT's Driver Plugin, containing a stealthy and surprisingly robust kernel-mode rootkit. Despite being abused by multiple operators, several variants remain validly signed, bypassing Microsoft's driver protections and loading successfully on the latest Windows builds. The rootkit's functionality — including coercive AV/EDR driver deletion, silent installation methods, and APC-based shellcode injection — demonstrates a level of sophistication rarely seen in malware distributed through public builders.

Our telemetry and detection work further expose a dramatic rise in ValleyRAT's presence in the wild. Roughly 85% of detected plugin samples surfaced within the past six months, directly following the builder leak. This surge marks a turning point: ValleyRAT is no longer a tool reliably associated with specific Chinese-speaking threat actors, but rather an accessible platform fueling opportunistic and un-attributable campaigns.

This research pulls back the curtain on ValleyRAT's internals, its kernel rootkit mechanics, and the implications of a powerful multi-module malware ecosystem becoming available to the masses. When sophisticated tooling escapes into the wild, who gets to wield it — and who pays the price?

SpeakerBio: Jiří Vinopal, Threat Researcher at Check Point Research

Jiří Vinopal is a security researcher, malware researcher, and reverse engineer at Check Point Research, focused on advanced cyber threats, kernel internals, and the hidden mechanics of undocumented system components. His work spans uncovering novel attack primitives, reconstructing proprietary protocols from binary analysis alone, and deep-diving into both sophisticated malware families and trusted platform components. When he's not buried in disassembly, he actively shares his knowledge and passion for reverse engineering across his X account, YouTube channel, and blog — delivering tips, tricks, and technical insights to fellow enthusiasts and the broader security community.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Maker's Village - Saturday - 13:00-13:59 PDT

Title: Crafting the Future: DEF CON 34 Light-Up Bow Workshop

Tags: Maker's Village | Hack3r Runw@y v8.0 | Creator Event/Activity

When: Saturday, Aug 8, 13:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 1 301 (Makers' Village) - [Map](#)

Description:

Level up your wearable tech skills and celebrate **DEF CON 34** by making your own interactive, light-up accessory! In this hands-on e-textile workshop, proudly presented by **Hack3r Runway**, you will learn the basics of wearable electronics and sewing circuits to create a custom glowing bow. Whether you want to rock it in your hair or wear it as a sleek cyberpunk bow tie, you'll walk away with a unique, handmade piece of hacker fashion. What you'll learn ***Intro to E-Textiles:** Learn how to design a basic circuit using a LilyPad battery holder and wearable LEDs. *** Conductive Thread Basics:** Master the art of hand-sewing with conductive thread to power your creation without bulky wires. *** Exclusive Swag:** Assemble your circuit onto a custom 3D-printed bow featuring a special **glow-in-the-dark DEF CON 34 logo**.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Contests - Saturday - 13:00-14:59 PDT

Title: Crash and Compile - Stage Competition

Tags: Crash and Compile | Contest

When: Saturday, Aug 8, 13:00 - 14:59 PDT

Where: LVCCW Level 1 Hall 1 100 (Contest Stage) - [Map](#)

Description:

What happens when you take an ACM style programming contest, smash it head long into a drinking game, throw in a mix of our most distracting helpers, then shove the resulting chaos on stage in front of an audience? You get the contest known as Crash and Compile.

Teams are given programming challenges and have to solve them with code. If your code fails to compile? Take a drink. Segfault? Take a drink. Did your code fail to produce the correct answer when you ran it? Take a drink. ChatGPT wrote your code? First of all shame. Secondly take a drink.

We set you against the clock and the other teams. And because our "Team Distraction" think watching people simply code is boring, they have taken it upon themselves to be creative in hindering you from programming, much to the enjoyment of the audience. At the end of the night, one team will have proven their ability, and walk away with the coveted Crash and Compile trophy.

Crash and Compile is looking for the top programmers to test their skills in our contest. Can you complete our challenges? Can you do so with style that sets your team ahead of the others? To play our game you must first complete our qualifying round. Gather your team and see if you have the coding chops to secure your place as one of the top teams to move on to the main contest.

Qualifications for Crash and Compile will take place Friday starting at 10:00 and run till 18:00, both in the contest area and online at <https://crashandcompile.org>

You may have up to two people per team. Individuals can compete, but having two people on a team is highly suggested.

Of the qualifiers, ten teams will move on to compete head to head on the contest stage on Saturday.

Participant Prerequisites

As this contest involves the drinking of alcohol (beer), all contestants must be 21 years of age or older. Yes we will check. While we don't limit what development environment or programming language you chose to use, as we used a PDP11/23 when we competed, the team must have at least one computer that can connect to our contest network via wired ethernet for the main contest.

Pre-Qualification

Qualifiers run on Friday from 10:00 to 18:00. We will be located in the contest area, and the problems can be accessed via our site at <https://crashandcompile.org>

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Crashing the Party: Pwning Control-Flow Integrity with Segmentation Fault-Oriented Programming

Tags: DEF CON Official Talk | Demo | Tool | Exploit

When: Friday, Aug 7, 11:30 - 12:30 PDT

Where: LVCCW Level 1 Hall 3 1007 (Main Track 2) - [Map](#)

Description:

A program crashes with a segmentation fault. Then, it crashes again. And again. What looks like crazy behaviour is actually an exploit, running one crash at a time.

In this talk, we present Segmentation Fault-Oriented Programming (SFOP), a novel exploitation technique that weaponizes 12 previously unknown weaknesses in the Linux kernel's handling of signals to execute arbitrary code. SFOP is designed to bypass Intel CET, the most widely deployed hardware Control-Flow Integrity (CFI) scheme on modern x86-64 systems, built to stop classic code-reuse attacks such as Return-Oriented Programming (ROP) and Sigreturn-Oriented Programming (SROP). Unlike previous CFI bypass techniques, SFOP is a general-purpose technique that can by-default reliably exploit any vulnerable x86-64 application with Intel CET enabled, becoming the lowest-hanging fruit attack after Intel CET.

We will show how SFOP bypasses CFI and turns a single memory-corruption vulnerability into arbitrary code execution on real-world targets. Through practical exploits, we demonstrate that what appears to be a process trapped in a crash loop is, in reality, attacker-controlled execution progressing fault by fault. Finally, we discuss the underlying weaknesses that make SFOP possible and the mitigations needed to defend against this new class of attacks.

Our paper has a ~50 references, like most academic papers. We have references to the Linux kernel lines that showcase the vulnerabilities we find, even! Here we copy paste our references, but everything is properly ordered in the paper.

[1] LMS Phrack 40. Bypassing cet & bti with functional oriented programming. https://phrack.org/issues/71/7_md. (29-10-2025). [2] Martin Abadi, Mihai Budiu, Ulfar Erlingsson, and Jay Ligatti. Control-flow integrity. In Proceedings of the 12th ACM Conference on Computer and Communications Security, CCS '05, page 340–353, New York, NY, USA, 2005. Association for Computing Machinery. [3] Marcos Bajo and Christian Rossow. Await() a second: evading control flow integrity by hijacking c++ coroutines. In Proceedings of the 34th USENIX Conference on Security Symposium, SEC '25, USA, 2025. USENIX Association. [4] Markus Bauer, Ilya Grishchenko, and Christian Rossow. Typro: Forward cfi for c-style indirect function calls using type propagation. In Proceedings of the 38th Annual Computer Security Applications Conference, ACSAC '22, page 346–360, New York, NY, USA, 2022. Association for Computing Machinery. [5] Lucas Becker, Matthias Hollick, and Jiska Classen. Sok: on the effectiveness of control-flow integrity in practice. In Proceedings of the 18th USENIX Conference on Offensive Technologies, WOOT'24, USA, 2024. USENIX Association. [6] Lorenzo Binosi, Gregorio Barzasi, Michele Carminati, Stefano Zanero, and Mario Polino. The Illusion of Randomness: An Empirical Analysis of Address Space Layout Randomization Implementations. In Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security, 2024. [7] Tyler Bletsch, Xuxian Jiang, Vince W. Freeh, and Zhenkai Liang. Jump-oriented programming: A new class of code-reuse attack. In Proceedings of the ACM Symposium on Information, Computer and Communications Security, ASIACCS, 2011. [8] Erik Bosman. x86: Srop mitigation: implement signal counting. <https://lkml.org/lkml/2014/5/15/858>. (12-11-2025). [9] Erik Bosman and Herbert Bos. Framing signals - a return to portable shellcode. In 2014 IEEE Symposium on Security and Privacy, pages 243–258, 2014. [10] Nicholas Carlini, Antonio Barresi, Mathias Payer, David Wagner, and Thomas R. Gross. Control-Flow bending: On the effectiveness of Control-Flow integrity. In 24th USENIX Security Symposium (USENIX Security 15), pages 161–176, Washington, D.C., August 2015. USENIX Association. [11] Chromium. syscall sets.cc - chromium github. https://github.com/chromium/chromium/blob/main/sandbox/linux/seccomp-bpf-helpers/syscall_sets.cc#L353. (12-11-2025). [12] Exploit Database. Nginx 1.3.9 - 1.4.0 - chunked encoding stack buffer overflow (metasploit). <https://www.exploit-db.com/exploits/25775>. (29-10-2025). [13] V8 Developers. Control-flow integrity in v8. <https://v8.dev/blog/control-flow-integrity>. (29-10-2025). [14] Docker Docs. Seccomp security profiles for docker. <https://docs.docker.com/engine/security/seccomp/>. (12-11-2025). [15] Victor Duta, Fabian Freyer, Fabio Pagani, Marius Muench, and Cristiano Giuffrida. Let me unwind that for you: Exceptions to backward-edge protection. In Symposium on

Network and Distributed System Security (NDSS), 2023. [16] Mozilla Firefox. Sandboxfilter.cpp - firefox github. <https://github.com/mozilla-firefox/firefox/blob/main/security/sandbox/linux/SandboxFilter.cpp#L1178>. (12-11-2025). [17] Alexander J. Gaidis, Joao Moreira, Ke Sun, Alyssa Milburn, Vaggelis Atlidakis, and Vasileios P. Kemerlis. Fineibt: Fine-grain control-flow enforcement with indirect branch tracking. In Proceedings of the 26th International Symposium on Research in Attacks, Intrusions and Defenses, RAID '23, page 527–546, New York, NY, USA, 2023. Association for Computing Machinery. [18] GNU. Gcc wiki - vtv. <https://gcc.gnu.org/wiki/vtv>. (12-11-2025). [19] GNU. Program instrumentation options. <https://gcc.gnu.org/onlinedocs/gcc/Instrumentation-Options.html>. (12-11-2025). [20] Yingjie Guo, Liwei Chen, and Gang Shi. Function-oriented programming: A new class of code reuse attack in c applications. In 2018 IEEE Conference on Communications and Network Security (CNS), pages 1–9, 2018. [21] Enes Goktas, Elias Athanasopoulos, Herbert Bos, and Georgios Portokalidis. Out of control: Overcoming control-flow integrity. In 2014 IEEE Symposium on Security and Privacy, pages 575–589, 2014. [22] Hong Hu, Zheng Leong Chua, Sendriou Adrian, Prateek Saxena, and Zhenkai Liang. Automatic generation of Data-Oriented exploits. In 24th USENIX Security Symposium (USENIX Security 15), pages 177–192, Washington, D.C., August 2015. USENIX Association. [23] Hong Hu, Shweta Shinde, Sendriou Adrian, Zheng Leong Chua, Prateek Saxena, and Zhenkai Liang. Data-oriented programming: On the expressiveness of non-control data attacks. In 2016 IEEE Symposium on Security and Privacy (SP), pages 969–986, 2016. [24] Intel. A technical look at intel® control-flow enforcement technology. <https://www.intel.com/content/www/us/en/developer/articles/technical/technical-look-control-flow-enforcement-technology.html>. (29-10-2025). [25] Seunghoon Jeong, Jaejoon Hwang, Hyukjin Kwon, and Dongkyoo Shin. A cfi countermeasure against got overwrite attacks. IEEE Access, 8:36267–36280, 2020. [26] Linux Kernel. Control-flow enforcement technology (cet) shadow stack. <https://docs.kernel.org/arch/x86/shstk.html>. (12-11-2025). [27] LLVM. Control flow integrity design documentation. <https://clang.llvm.org/docs/ControlFlowIntegrityDesign.html>. (12-11-2025). [28] Linux manual page. Sigaction(2) - linux manual page. <https://man7.org/linux/man-pages/man2/sigaction.2.html>. (05-10-2025). [29] Ben Niu and Gang Tan. Modular control-flow integrity. In Proceedings of the 35th ACM SIGPLAN Conference on Programming Language Design and Implementation, PLDI '14, page 577–587, New York, NY, USA, 2014. Association for Computing Machinery. [30] PaX. Address space randomization. <https://pax.grsecurity.net/docs/aslr.txt>, 2003. (12-11-2025). [31] Aravind Prakash, Xunchao Hu, and Heng Yin. vfguard: Strict protection for virtual function calls in cots c++ binaries. In Proceeding of the Annual Network and Distributed System Security Symposium (NDSS), 01 2015. [32] Bootlin Elixir Cross Referencer. create rstor token (linux kernel source code). <https://elixir.bootlin.com/linux/v6.15.2/source/arch/x86/kernel/shstk.c#L64>. (29-10-2025). [33] Bootlin Elixir Cross Referencer. get shstk data (linux kernel source code). <https://elixir.bootlin.com/linux/v6.15.2/source/arch/x86/kernel/shstk.c#L272>. (29-10-2025). [34] Bootlin Elixir Cross Referencer. libc sigaction (glibc source code). <https://elixir.bootlin.com/glibc/glibc-2.33/source/sysdeps/unix/sysv/linux/sigaction.c#L42>. (29-10-2025). [35] Bootlin Elixir Cross Referencer. pte mkwrite shstk (linux kernel source code). <https://elixir.bootlin.com/linux/v6.15.2/source/arch/x86/include/asm/pgtable.h#L491>. (29-10-2025). [36] Bootlin Elixir Cross Referencer. rt sigaction (linux kernel source code). <https://elixir.bootlin.com/linux/v6.15.7/source/kernel/signal.c#L4644>. (29-10-2025). [37] Bootlin Elixir Cross Referencer. rt sigreturn l266 (linux kernel source code). https://elixir.bootlin.com/linux/v6.15.2/source/arch/x86/kernel/signal_64.c#L266. (29-10-2025). [38] Bootlin Elixir Cross Referencer. rt sigreturn l275 (linux kernel source code). https://elixir.bootlin.com/linux/v6.15.2/source/arch/x86/kernel/signal_64.c#L275. (29-10-2025). [39] Bootlin Elixir Cross Referencer. setup signal shadow stack l364 (linux kernel source code). <https://elixir.bootlin.com/linux/v6.15.2/source/arch/x86/kernel/shstk.c#L364>. (29-10-2025). [40] Bootlin Elixir Cross Referencer. setup signal shadow stack l370 (linux kernel source code). <https://elixir.bootlin.com/linux/v6.15.2/source/arch/x86/kernel/shstk.c#L370>. (29-10-2025). [41] Bootlin Elixir Cross Referencer. Sigaction (linux kernel source code). <https://elixir.bootlin.com/linux/v6.15.2/source/arch/x86/include/uapi/asm/signal.h#L93>. (05-10-2025). [42] Bootlin Elixir Cross Referencer. Sigframe (linux kernel source code). <https://elixir.bootlin.com/linux/v6.15.2/source/arch/x86/include/asm/sigframe.h#L59>. (05-10-2025). [43] Bootlin Elixir Cross Referencer. sigset t (glibc source code). https://elixir.bootlin.com/glibc/glibc-2.33/source/signal/bits/types/sigset_t.h#L7. (29-10-2025). [44] Bootlin Elixir Cross Referencer. sigset t (linux kernel source code). <https://elixir.bootlin.com/linux/v6.15.7/source/arch/x86/include/asm/signal.h#L25>. (29-10-2025). [45] AliAkbar Sadeghi, Salman Niksefat, and Maryam Rostamipour. Pure call oriented programming (pcop): chaining the gadgets using call instructions. Journal of Computer Virology and Hacking Techniques, 14:1–18, 05 2018. [46] Felix Schuster, Thomas Tendyck, Christopher Liebchen, Lucas Davi, Ahmad-Reza Sadeghi, and Thorsten Holz. Counterfeit object-oriented programming: On the difficulty of preventing code reuse attacks in c++ applications. In Proceedings of the IEEE Symposium on Security and Privacy, SP, 2015. [47] Hovav Shacham. The geometry of innocent flesh on the bone: Return-into-libc without function calls (on the x86). In Proceedings of the ACM conference on Computer and Communications Security, CCS,

2007. [48] sroettger. Ierae ctf 2024. <https://gist.github.com/sroettger/fe66f7eb0cb10a8ebd1454875a7131ea>. (29-10-2025). [49] Ubuntu. Compilerflags - ubuntu wiki. <https://wiki.ubuntu.com/ToolChain/CompilerFlags>. (29-10-2025). [50] Chao Zhang, Scott A. Carr, Tongxin Li, Yu Ding, Chenyu Song, Mathias Payer, and Dawn Song. Vtrust: Regaining trust on virtual calls. In Proceedings of the Annual Network and Distributed System Security Symposium (NDSS), 2016. [51] Tianning Zhang, Miao Cai, Diming Zhang, and Hao Huang. esrop attack: Leveraging signal handler to implement turing-complete attack under cfi defense. In Fengjun Li, Kaitai Liang, Zhiqiang Lin, and Sokratis K. Katsikas, editors, Security and Privacy in Communication Networks, pages 752–769, Cham, 2023. Springer Nature Switzerland

Speakers: Marcos "h3xduck" Bajo, Ritvik "RoYalGamr" Goyal

SpeakerBio: Marcos "h3xduck" Bajo, CISA Helmholtz Center for Information Security

Marcos Bajo aka h3xduck is a security researcher and PhD student at the CISA Helmholtz Center for Information Security in Germany. His research focuses on exploitation techniques and malware, but more broadly, he's interested in breaking things others build—and building things to break things.

SpeakerBio: Ritvik "RoYalGamr" Goyal

Ritvik Goyal is a Senior Undergraduate in Mathematics and Scientific Computing at the Indian Institute of Technology Kanpur. He recently worked as a Research Intern at the CISA Helmholtz Center, focusing on system security research regarding Control Flow Integrity protections like Intel CET. He is a key member of the competitive CTF team Wiredin IITK and actively mentors students in cybersecurity at Programming Club IIT Kanpur.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Red Team Village - Saturday - 14:00-15:59 PDT

Title: Crawlee - Improving crawling with an LLM

Tags: Red Team Village | Misc

When: Saturday, Aug 8, 14:00 - 15:59 PDT

Where: LVCCW Level 1 Hall 1 309 (Red Team Village) Tactic Table 1 - [Map](#)

Description:

Traditional web crawlers are great at finding links but terrible at understanding websites. The interesting challenge is not replacing crawlers with AI. It's using the minimum amount of AI required to dramatically improve coverage.

Every automated tool I've tried hit a brick wall the moment it encounters MFA, multi-step workflows, onboarding wizards, or application states where a wrong click deletes data. As a result, large portions of authenticated attack surface require manually using the application.

I built a crawler that combines deterministic tooling such as Katana with a minimal AI agent. The AI is only used where traditional crawlers consistently fail: authentication, workflow navigation, and generation of safety controls. Once authenticated session state is established, the system hands control back to fast deterministic tooling.

I'll cover the basics of how it's built and we'll try it together on a variety of applications.

SpeakerBio: Daniel Goldberg

Daniel is a security researcher who spent the last 20 years crawling his way up the stack from hacking operating systems to attacking client-side applications to attacking browsers, network protocols, and today web applications. After dabbling with everything in security, he's realized what he really enjoys is how to take something that works and make it really good

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Scambait Village - Saturday - 15:30-16:59 PDT

Title: Creator Drop-In

Tags: Scambait Village | Creator Event/Activity

When: Saturday, Aug 8, 15:30 - 16:59 PDT

Where: LVCCW Level 1 Hall 1 208 (Scambait Village) - [Map](#)

Description:

We know a handful of names you would recognize are wandering this conference. We have invited them to swing by the village during this block and say hi. No stage, no line, no format. Just a shot at an actual conversation with the people behind the calls, so ask what you have always wanted to ask and swap a few stories of your own.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Scambait Village - Saturday - 14:00-15:30 PDT

Title: Creator Talk with RinoaPoison & VanHelen

Tags: Scambait Village | Creator Talk/Panel

When: Saturday, Aug 8, 14:00 - 15:30 PDT

Where: LVCCW Level 1 Hall 1 208 (Scambait Village) - [Map](#)

Description:

Join popular scambait content creators RinoaPoison and VanHelen for an open, behind-the-scenes conversation about live scambaiting, character work, community building, and the realities of turning the tables on scammers on Twitch and YouTube. Expect stories from the calls, tips for aspiring creators, and insights into keeping the work sustainable and entertaining while still disrupting scam operations.

Speakers:RinoaPoison,VanHelen

SpeakerBio: RinoaPoison, Twitch Streamer / Content Creator

No BIO available

SpeakerBio: VanHelen, Twitch Streamer / Content Creator

No BIO available

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: CRLF-Powered Desync Attacks: Beheading HTTP streams

Tags: DEF CON Official Talk | Demo | Tool | Exploit

When: Saturday, Aug 8, 17:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 3 906 (Main Track 3) - [Map](#)

Description:

Have you ever discovered a header injection vulnerability and settled for little more than an open redirect or XSS? In this session, we introduce a battle-tested “header injection” powered desync methodology, enabling you to perform HTTP request smuggling attacks against even strictly RFC-compliant proxy chains.

We will begin by explaining a well-known but overlooked CRLF injection primitive that produced HTTP Request Splitting inside the core infrastructure of a major CDN, resulting in the capture of live users’ credentials across thousands of compromised applications.

Building upon this, we’ll demonstrate how header injections can be used to exploit more traditional smuggling attack classes, even when no parser discrepancy exists. Finally we’ll reveal how you can shift previously non-compliant desync attacks into the browser, unlocking a plethora of novel exploitation opportunities even when keep-alive connections are not shared between users. The result is a slew of real-world case studies with impacts ranging from account takeovers via desync-enabled XSS gadgets to cache poisoning, response queue poisoning, access control bypasses, and in several cases the possibility of creating the ever-terrifying desync worm.

Finally, we’ll release two open source tools that introduce robust detection of header injection.

Speakers: Tom "t0xodile" Stacey, Tobia "mastersplinter" Righi

SpeakerBio: Tom "t0xodile" Stacey, Independent

Tom 't0xodile' Stacey is a security researcher at PortSwigger with a passion for automating the ideas that "will never work" to find gaps in the industry's current understanding of web security. He is best known for his work in discovering and exploiting underappreciated forms of desync attacks.

At PortSwigger he spends most of his time experimenting with the HTTP protocol and the vulnerabilities that arise due to the disagreements between web servers and components with the goal of finding novel techniques to improve Burp Suite's capabilities. When he's not at work, he's usually playing some form of video / board game or building Lego.

SpeakerBio: Tobia "mastersplinter" Righi, TurtleSec

I am a security research and bug bounty hunter, recently I have started TurtleSec with other talented hackers, focusing on research driven projects. I spend most of my time tinkering with applications to try and figure out how to break them in the weirdest of ways.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Cryptid Hunt

Tags: Cryptid Hunt | Contest

When: Sunday, Aug 9, 10:00 - 11:59 PDT

Where: LVCCW Level 1 Hall 1 203 (Cryptid Hunt) - [Map](#)

Description:

Something is already watching you.

The Cryptid Hunt is a task-oriented challenge that moves agents across the conference floor toward a truth most attendees will never find. This is not a passive experience — each clue demands action, and the path forward is never obvious.

Look carefully at what surrounds you. The next layer of any good mystery is always hiding beneath the surface. Patterns emerge for those paying attention. Signals exist for those who know how to listen.

Is this a puzzle? A test? A hunt? At its core, this is a community experience that rewards curiosity, persistence, and the willingness to go further than most people will.

The conference is your map. Maritime exploration, ancient communication, and the village of knowledge surrounding you are all part of the journey. Nothing here is coincidental.

Finishers are recognized. What awaits those who complete the hunt will not be found anywhere else at this conference. Supplies are finite. So is your time.

Your first clue is already in your hands.

— The Cryptid Hunt Team

Bureau of Unverified Phenomena · DC34

Participant Prerequisites

- Smart Phone
- Desire to Learn
- Patience

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Cryptid Hunt

Tags: Cryptid Hunt | Contest

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 203 (Cryptid Hunt) - [Map](#)

Description:

Something is already watching you.

The Cryptid Hunt is a task-oriented challenge that moves agents across the conference floor toward a truth most attendees will never find. This is not a passive experience — each clue demands action, and the path forward is never obvious.

Look carefully at what surrounds you. The next layer of any good mystery is always hiding beneath the surface. Patterns emerge for those paying attention. Signals exist for those who know how to listen.

Is this a puzzle? A test? A hunt? At its core, this is a community experience that rewards curiosity, persistence, and the willingness to go further than most people will.

The conference is your map. Maritime exploration, ancient communication, and the village of knowledge surrounding you are all part of the journey. Nothing here is coincidental.

Finishers are recognized. What awaits those who complete the hunt will not be found anywhere else at this conference. Supplies are finite. So is your time.

Your first clue is already in your hands.

— The Cryptid Hunt Team

Bureau of Unverified Phenomena · DC34

Participant Prerequisites

- Smart Phone
- Desire to Learn
- Patience

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Cryptid Hunt

Tags: Cryptid Hunt | Contest

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 203 (Cryptid Hunt) - [Map](#)

Description:

Something is already watching you.

The Cryptid Hunt is a task-oriented challenge that moves agents across the conference floor toward a truth most attendees will never find. This is not a passive experience — each clue demands action, and the path forward is never obvious.

Look carefully at what surrounds you. The next layer of any good mystery is always hiding beneath the surface. Patterns emerge for those paying attention. Signals exist for those who know how to listen.

Is this a puzzle? A test? A hunt? At its core, this is a community experience that rewards curiosity, persistence, and the willingness to go further than most people will.

The conference is your map. Maritime exploration, ancient communication, and the village of knowledge surrounding you are all part of the journey. Nothing here is coincidental.

Finishers are recognized. What awaits those who complete the hunt will not be found anywhere else at this conference. Supplies are finite. So is your time.

Your first clue is already in your hands.

— The Cryptid Hunt Team

Bureau of Unverified Phenomena · DC34

Participant Prerequisites

- Smart Phone
- Desire to Learn
- Patience

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

The Diana Initiative - Saturday - 10:20-10:30 PDT

Title: Crypto And Privacy Village Tour

Tags: The Diana Initiative | Creator Tour

When: Saturday, Aug 8, 10:20 - 10:30 PDT

Where: LVCCW Level 1 South Lobby / Atrium - [Map](#)

Description:

Interested in visiting Crypto And Privacy Village but afraid to go by yourself? The Diana Initiative is hosting tours! Follow a volunteer to Crypto And Privacy Village and be introduced to the community and activities inside!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Crypto Is Fine. The Code Is Not: Real-World Cryptographic Failures

Tags: Crypto & Privacy Village | Creator Talk/Panel

When: Friday, Aug 7, 16:30 - 17:15 PDT

Where: LVCCW Level 1 Hall 3 801 (Creator Stage 2) - [Map](#)

Description:

Developers keep getting crypto wrong in the same ways. Not the math, but the code around it. A missing check here, implicit trust there, and suddenly a signature means nothing. This talk is data-driven and hands-on. Starting from OWASP A04:2025, we examine real CVEs from GitHub Security Advisories as of January 2026 to show which crypto failure patterns actually dominate in the wild, then go deep on the top two: signature verification bypasses (including invalid curve attacks) and algorithm confusion bugs (JWT). Real libraries, live exploits. Demos and CTF challenges are woven throughout, involves audience interaction and participation. No crypto background required.

SpeakerBio: Diptendu Kar

Diptendu Kar is a security researcher focused on supply chain and dependency risk. He works on triaging open-source vulnerabilities, writing detection rules, and exploring how AI can automate tedious parts of security research. He also teaches Software Security Practices at Northeastern University part time and holds a Master's in Cybersecurity. Before security, he worked as a Java developer at TCS. He is especially interested in patch diffing, vulnerable function detection, and the use of LLMs in AppSec. He believes cryptography is magic and AI is a noisy intern - helpful but always needs supervision.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Cryptocurrency Closing Keynote

Tags: Cryptocurrency Village | Creator Talk/Panel

When: Sunday, Aug 9, 11:00 - 11:59 PDT

Where: LVCCW Level 1 Hall 3 1103 (Creator Stage 5) - [Map](#)

Description:

Closing the Cryptocurrency areas at DEFCON, we introduce everyone at work and their achievements during the event. We review our four major activities including the hackathon, contests, workshops, and capture the flag competition. A summary of teams, winners, and statistics indicates the degree of participation in this event. We describe what prizes were awarded and which contestants won big. A list of workshop topics follows, with instructors giving their impressions of how modern finance technology benefits from interactive learning. Finally, we give a sneak preview of what's to come in the Cryptocurrency areas (Village, Contest, Vendor, Party, Training) at DEFCON in Bahrain and how we intend to fulfill the mandate of fostering cryptocurrency exploration and hacking there.

Speakers: Chelsea Button, Param "P7R7M", Arjun "Peper" Suresh

SpeakerBio: Chelsea Button, Cryptocurrency Education Initiative

Chelsea is a lawyer specializing in consumer finance, data and technology. She advises clients on updates in the law and defends them in litigation. She is a cryptocurrency advocate, with multiple professional publications.

SpeakerBio: Param "P7R7M"

Param is an Electrical Engineering Student from Georgia Tech with a strong passion for and interest in crypto. Although he primarily got interested in cryptography and hardware security through a class at Georgia Tech, he is also working at a software company on crypto adoption and ease of use. With a unique blend of HW and SW skills, Param is truly enthusiastic about all aspects of crypto.

SpeakerBio: Arjun "Peper" Suresh, Postgraduate Student, University of Wollongong in Dubai

Arjun Suresh is pursuing postgraduate studies in Cybersecurity at the University of Wollongong in Dubai, specializing in blockchain security, penetration testing, and applied cryptography. His interest in crypto security was shaped by analyzing major exchange breaches, including the Mt. Gox and Ronin Network hacks, where he studied the gap between attacker tradecraft and real-world defenses.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Cryptocurrency Opening Keynote

Tags: Cryptocurrency Village | Creator Talk/Panel

When: Friday, Aug 7, 11:00 - 11:59 PDT

Where: LVCCW Level 1 Hall 3 1103 (Creator Stage 5) - [Map](#)

Description:

Join your fellow hackers managing the Cryptocurrency areas at DEF CON, and get a sneak peak of what each workshop teaches as well as an overview of the showcases and programs happening in our DEF CON Village and Contest areas. We will report on cryptocurrency trends and perspectives from distinguished positions in industry, academy, and government. We will announce the teams competing in the Cryptocurrency Challenge, and give an overview of what prizes are available to winning contestants of the hackathon, CTF, and contests. Meet the organizers of years of cryptocurrency content at Defcon and bring your questions to the Creator Stage during the Cryptocurrency Opening Keynote!

Speakers:Michael "MsvB" Schloh,Param "P7R7M",Arjun "Peper" Suresh

SpeakerBio: Michael "MsvB" Schloh, Chairman, Monero Devices

The Cryptocurrency Advocate is a group working to prepare society for the likely adoption of modern cryptocurrency in legacy financial systems. We host a number of events, including the Cryptocurrency Village and Cryptocurrency Challenge at DEFCON hacker conventions and other cybersecurity events around the world.

SpeakerBio: Param "P7R7M"

Param is an Electrical Engineering Student from Georgia Tech with a strong passion for and interest in crypto. Although he primarily got interested in cryptography and hardware security through a class at Georgia Tech, he is also working at a software company on crypto adoption and ease of use. With a unique blend of HW and SW skills, Param is truly enthusiastic about all aspects of crypto.

SpeakerBio: Arjun "Peper" Suresh, Postgraduate Student, University of Wollongong in Dubai

Arjun Suresh is pursuing postgraduate studies in Cybersecurity at the University of Wollongong in Dubai, specializing in blockchain security, penetration testing, and applied cryptography. His interest in crypto security was shaped by analyzing major exchange breaches, including the Mt. Gox and Ronin Network hacks, where he studied the gap between attacker tradecraft and real-world defenses.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

The Diana Initiative - Friday - 12:20-12:30 PDT

Title: Cryptocurrency Village Tour

Tags: The Diana Initiative | Creator Tour

When: Friday, Aug 7, 12:20 - 12:30 PDT

Where: LVCCW Level 1 South Lobby / Atrium - [Map](#)

Description:

Interested in visiting Cryptocurrency Village but afraid to go by yourself? The Diana Initiative is hosting tours! Follow a volunteer to Cryptocurrency Village and be introduced to the community and activities inside!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Cryptographer Recruitment: Crack the Substitution Cipher

Tags: DCNextGen | Creator Event/Activity | Youth

When: Friday, Aug 7, 12:00 - 12:45 PDT

Where: LVCCW Level 3 W316 (DC NextGen) - [Map](#)

Description:

You're a Cryptographer When Jumbled Letters are Exciting, Not Scary! The substitution cipher is a game of mathematics and patterns. With basic skills (or online tools) ciphers are easy to decipher. Don't let them fool you! Attendees will need some paper, a writing device, and access to the Substitutor web app.

SpeakerBio: Bradán Lane

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Cryptohack Badge Hacking

Tags: Cryptocurrency Village | Creator Talk/Panel

When: Friday, Aug 7, 14:00 - 14:59 PDT

Where: LVCCW Level 1 Hall 3 1103 (Creator Stage 5) - [Map](#)

Description:

In this hour, we'll guide you from setup to exploitation of a Cryptohack electronic badge. From installing the ESP-IDF toolchain, understanding application logic, compiling and disassembling firmware, we get familiar with the basics before considering the advanced aspects of financial technology in hardware. To explore the typical interfaces of a hardware wallet, we experiment with live hacks on a testnet wallet supporting Solana, Ethereum, Bitcoin, and Monero. By the end of the session, you'll know how to probe the boundaries of hardware security and leave with insights you can apply to real-world offensive security challenges.

Speakers: Do Truong Giang "FSNaix", Sadiq "Sdqmd", Arjun "Peper" Suresh

SpeakerBio: Do Truong Giang "FSNaix", BlossomsAI / Bloomify (AI & Security)

I'm Giang (FSNaix), an AI and security researcher from Vietnam and a Bloomify cofounder. I help build open-source Vietnamese language models with BlossomsAI, I built Petal (an AI tool that reverse-engineers binaries faster than doing it by hand), and at DEFCON Singapore 1 I managed to get DOOM running on a \$20 conference badge.

SpeakerBio: Sadiq "Sdqmd", CodeBit

sdqmd (Sadiq) is a hardware hacker and co-founder of CodeBit, a technology company based in Brunei that's building a hardware engineering academy to teach embedded systems and security from the ground up. He is focused on developing a pedagogy that blends theory with hands-on practice, so aspiring hackers — especially those just starting out — don't just learn how something works; they build it, break it, and understand it for themselves. His own research focuses on hardware attacks against embedded devices — using fault injection and power analysis to defeat the security of everything from crypto hardware wallets to point-of-sale infrastructure. Above all, he's driven by one goal: building hardware and security competency in Brunei, where hands-on learning is still hard to come by.

SpeakerBio: Arjun "Peper" Suresh, Postgraduate Student, University of Wollongong in Dubai

Arjun Suresh is pursuing postgraduate studies in Cybersecurity at the University of Wollongong in Dubai, specializing in blockchain security, penetration testing, and applied cryptography. His interest in crypto security was shaped by analyzing major exchange breaches, including the Mt. Gox and Ronin Network hacks, where he studied the gap between attacker tradecraft and real-world defenses.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

OSINT For Good Community - Saturday - 11:15-11:45 PDT

Title: CTF Intro, Quick Guides, and Rule Review

Tags: OSINT For Good Community | Creator Talk/Panel

When: Saturday, Aug 8, 11:15 - 11:45 PDT

Where: LVCCW Level 1 Hall 4 1307 (OSINT4Good Community) Stage - [Map](#)

Description:

Participating in today's Global OSINT Search Party CTF? This session, offered by our most senior Coach, the Legendary KennyJ, will do a quick overview of what to expect, how to get organized, and how to make sure you're following the rules.

SpeakerBio: Kenny J, Trace Labs

Senior Infrastructure Engineer by day. Osint for Good by night. His is the only Trace Labs coach to have coached 20+ CTFs, earning him the singular rank of Legendary Coach.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Noob Community - Sunday - 10:30-11:30 PDT

Title: Ctrl + Alt + Lead: Rebooting Cyber Culture with Human Skills

Tags: Noob Community | Creator Talk/Panel

When: Sunday, Aug 9, 10:30 - 11:30 PDT

Where: LVCCW Level 1 Hall 4 1417 (Noob Community) - [Map](#)

Description:

Session Description: Technical skills might open doors in IT & Cybersecurity, but leadership, communication, and mentorship sustain growth and impact. As the field becomes more complex and critical, we must rethink how we build and lead teams.

This talk highlights the soft skills that turn strong technicians into effective collaborators, trusted advisors, and emerging leaders: from coaching junior analysts to translating between the SOC and the C-suite.

Takeaways: Attendees will learn practical ways to foster teambuilding, conflict resolution, psychological safety, build mentorship pipelines, and communicate with clarity under pressure.

Target audiences: Everyone

SpeakerBio: Amanda Kollmorgan

No BIO available

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Blacks In Cyber Village - Friday - 13:00-13:55 PDT

Title: CTRL the Chaos: When AI Controls Critical Infrastructure

Tags: Blacks In Cyber Village | Creator Talk/Panel

When: Friday, Aug 7, 13:00 - 13:55 PDT

Where: LVCCW Level 3 W322-W324 (BIC Village) - [Map](#)

Description:

As artificial intelligence shifts from supporting analytics to exercising real-time operational control in critical infrastructure energy grids, aviation systems, healthcare networks, transportation, and national logistics it ceases to be a tool and becomes part of the infrastructure itself. AI now optimizes load balancing, automates routing, manages predictive maintenance, and drives high-stakes decisions that directly impact public safety, economic stability, and national security. This session introduces the CTRL framework (Control, Resilience, Trust, Leadership) a strategic blueprint for securing autonomous systems before they evolve into systemic risk. Drawing from hands-on experience in federal cybersecurity, aviation security, AI governance, and academic cybersecurity instruction, Nykolas Muldrow explores how AI expands the attack surface through threats like data poisoning, model drift, prompt injection, and compromised AI supply chains. Attendees will gain: A clear view of how embedded AI transforms infrastructure vulnerabilities A practical threat model tailored to autonomous operational systems Governance strategies aligned with NIST AI Risk Management Framework and ISO-based controls The CTRL leadership model for embedding responsible AI oversight into organizational strategy An immediate-use risk-evaluation method for their own products, infrastructure, or agencies In an era where regulators intensify scrutiny, investors demand deeper risk diligence, and operators race to deploy AI without proportional safeguards, the next decade of progress will belong to those who govern autonomous systems responsibly not just those who deploy them fastest. Join to equip yourself with the tools to lead before AI makes decisions we cannot easily reverse.

SpeakerBio: Nykolas Muldrow, CEO of CI Solutions Global Inc.

Nykolas Muldrow is a cybersecurity executive, CEO of CI Solutions Global Inc., and 2025 GovTechCon Mission Trailblazer Award recipient for their pioneering work in AI, cybersecurity, and secure cloud technologies for critical infrastructure. With 15+ years securing defense, aviation, and federal systems including aviation GRC at American Airlines they specialize in threat modeling autonomous AI in high-stakes environments like energy grids, transportation, and healthcare networks. Nyk teaches cybersecurity, aligns solutions to NIST AI RMF and ISO controls, and equips leaders to govern AI responsibly before it becomes systemic risk.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: CUDA've done better - Hacking Nvidia GPUs for container-escape and privilege escalation

Tags: DEF CON Official Talk | Demo | Exploit

When: Sunday, Aug 9, 12:30 - 13:30 PDT

Where: LVCCW Level 1 Hall 3 906 (Main Track 3) - [Map](#)

Description:

CUDA've done better - Hacking Nvidia GPUs for container-escape and privilege escalation. We found and exploited a UAF in the NVIDIA Linux kernel module that allows us to escape NVIDIA containers and gain root access on the host. We'll show novel exploitation techniques: bypass kernel heap mitigations, deterministically win races by abusing `rw_semaphore`, and execute code on the kernel without ever jumping anywhere (by writing directly to physical memory).

Speakers: Daniel "0xDACA" Cohen Hillel, Noam Trobishi

SpeakerBio: Daniel "0xDACA" Cohen Hillel

I used to be a vulnerability researcher for the army, but now that I'm a full time physics grad student researching superconducting quantum computers at the Weizmann Institute (very unrelated to hacking).

I just love hacking so much that I still do it in my spare time, while not doing physics. I like using hacking as an excuse to learn and deeply understand stuff. NVIDIA is a good example. I wanted to learn more about GPUs because of all the latest advancements in AI, so instead of seeing a tutorial/lecture about it, I just opened the code and started researching it. Another good example is when I hacked [Merkle trees](#) to learn more about zero-knowledge proofs.

SpeakerBio: Noam Trobishi, Atom

Noam is a low-level systems, GPU, and vulnerability researcher at Atom, where he works on GPU infrastructure for AI. He previously served in an IDF cyber unit and later worked as a vulnerability researcher at a private cybersecurity company. Noam holds a B.Sc. in Computer Science and Mathematics from the Hebrew University of Jerusalem and is currently pursuing a master's degree in Mathematics at the Hebrew University.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

DEF CON Training - Friday - 08:30-17:30 PDT

Title: Cyber & AI Policy Basics: What Every Organization Needs in Place

Tags: DEF CON Training (Paid) (1-day) | DEF CON Training

When: Friday, Aug 7, 08:30 - 17:30 PDT

Where: LVCCW Level 2 W223 (Training) - [Map](#)

Description:

Speakers:Pamela 'Pam' Feld,Greg Goldberg

SpeakerBio: Pamela 'Pam' Feld

No BIO available

SpeakerBio: Greg Goldberg

No BIO available

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Contests - Friday - 10:00-17:59 PDT

Title: Cyber Deck Competition

Tags: Maker's Village | Contest | Cyber Deck Makers' Contest

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 301 (Makers' Village) - [Map](#)

Description:

The cyber deck contest at DEF CON 34 encourages makers of all types to create their own cyber deck. Winners will be judged on form, function, creativity, does it work, general, awesomeness, and complexity.

Stop by Makers' Village for more info!

Judging Criteria

- Design Description
- Purpose
- Functionality
- Fancy-Do-Dads
- Processing Power
- Housing/Case utility
- Housing/Case Aesthetic Appeal
- Complexity
- Bonus categories revealed at con

Rules

1. Must be present to enter.
2. Winners are determined by points awarded by the judges.
3. Rules are subject to change.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Contests - Sunday - 10:00-11:59 PDT

Title: Cyber Deck Competition

Tags: Maker's Village | Contest | Cyber Deck Makers' Contest

When: Sunday, Aug 9, 10:00 - 11:59 PDT

Where: LVCCW Level 1 Hall 1 301 (Makers' Village) - [Map](#)

Description:

The cyber deck contest at DEF CON 34 encourages makers of all types to create their own cyber deck. Winners will be judged on form, function, creativity, does it work, general, awesomeness, and complexity.

Stop by Makers' Village for more info!

Judging Criteria

- Design Description
- Purpose
- Functionality
- Fancy-Do-Dads
- Processing Power
- Housing/Case utility
- Housing/Case Aesthetic Appeal
- Complexity
- Bonus categories revealed at con

Rules

1. Must be present to enter.
2. Winners are determined by points awarded by the judges.
3. Rules are subject to change.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Contests - Saturday - 10:00-17:59 PDT

Title: Cyber Deck Competition

Tags: Maker's Village | Contest | Cyber Deck Makers' Contest

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 301 (Makers' Village) - [Map](#)

Description:

The cyber deck contest at DEF CON 34 encourages makers of all types to create their own cyber deck. Winners will be judged on form, function, creativity, does it work, general, awesomeness, and complexity.

Stop by Makers' Village for more info!

Judging Criteria

- Design Description
- Purpose
- Functionality
- Fancy-Do-Dads
- Processing Power
- Housing/Case utility
- Housing/Case Aesthetic Appeal
- Complexity
- Bonus categories revealed at con

Rules

1. Must be present to enter.
2. Winners are determined by points awarded by the judges.
3. Rules are subject to change.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Blacks In Cyber Village - Saturday - 11:00-11:55 PDT

Title: Cyber Gamechangers: Women Who Lead, Secure, and Inspire

Tags: Blacks In Cyber Village | Creator Talk/Panel

When: Saturday, Aug 8, 11:00 - 11:55 PDT

Where: LVCCW Level 3 W322-W324 (BIC Village) - [Map](#)

Description:

Join B.I.C. Village for Cyber Gamechangers: Women Who Lead, Secure, and Inspire, a welcoming session focused on leadership, career growth, and the impact of women shaping cybersecurity. Come ready to learn, ask questions, and connect with the community.

Speakers: Nikkia Henderson, Arielle Baine, Jess Hoffman

SpeakerBio: Nikkia Henderson, Senior Advisor, Cybersecurity Infrastructure Security Agency (CISA) / President, Women in Cybersecurity Mid Atlantic Affiliate

Nikkia Henderson is a Senior Advisor at the Cybersecurity Infrastructure Security Agency (CISA), where they lead the Cyber Supply Chain Risk Management (C-SCRM) Strategy and Governance Program. They also serve as President of the Women in Cybersecurity Mid Atlantic Affiliate, helping professionals define their vision and career paths in federal cybersecurity. With over 14 years in federal government, Nikkia holds a Master's degree in Cyber Policy.

SpeakerBio: Arielle Baine, Chief of Cybersecurity at Cybersecurity and Infrastructure Security Agency (CISA)

Arielle Baine is the Chief of Cybersecurity for Region 3 within the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA). They lead the Cybersecurity Advisor Program, enhancing the security and resilience of critical infrastructure. With over 9 years of experience in cybersecurity across federal civilian and DoD communities, Arielle holds multiple certifications including CISSP, CCSP, GCWN, CEH, and Security+, and a Master of Science degree in Cybersecurity.

SpeakerBio: Jess Hoffman, Deputy CISO, City of Philadelphia / Professor, Harrisburg University and The Pennsylvania State University

Jess Hoffman is a Certified Information System Security Professional (CISSP) with nearly 20 years of IT and cybersecurity experience in government and private sectors, focusing on Audit and Compliance. They currently serve as Deputy CISO for the City of Philadelphia and are a Professor at Harrisburg University and The Pennsylvania State University. Jess is a national speaker and advocates for mentorship and DEI within cybersecurity.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

AI Village - Sunday - 10:00-13:59 PDT

Title: Cyber Mirage: Realtime Deepfake Demos

Tags: AI Village | Creator Event/Activity

When: Sunday, Aug 9, 10:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 2 603 (AI Village) - [Map](#)

Description:

Go deepfake yourself! This hands-on demo shows how threat actors leverage open-source deepfake video and voice cloning frameworks to impersonate anyone in realtime, conducting social engineering and compromising organizations using nothing more than a consumer-grade gaming laptop. No specialized hardware, no budget, no nation-state resources required. Come learn the tradecraft firsthand and find out just how convincing you can become.

SpeakerBio: Brandon Kovacs

Brandon Kovacs (CRT, OSCP) is a Senior Security Consultant at offensive cybersecurity firm Bishop Fox, where he specializes in red teaming, network penetration testing, and physical penetration testing. As a red team operator, he is adept at identifying critical attack chains that an external attacker could use to fully compromise organizations and reach high-value targets. Brandon is also recognized as a deepfake expert, conducting speaking sessions and live demonstrations at several global security and technology conferences. His research focuses on the intersection of offensive cybersecurity and artificial intelligence.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

AI Village - Friday - 10:00-17:59 PDT

Title: Cyber Mirage: Realtime Deepfake Demos

Tags: AI Village | Creator Event/Activity

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 2 603 (AI Village) - [Map](#)

Description:

Go deepfake yourself! This hands-on demo shows how threat actors leverage open-source deepfake video and voice cloning frameworks to impersonate anyone in realtime, conducting social engineering and compromising organizations using nothing more than a consumer-grade gaming laptop. No specialized hardware, no budget, no nation-state resources required. Come learn the tradecraft firsthand and find out just how convincing you can become.

SpeakerBio: Brandon Kovacs

Brandon Kovacs (CRT, OSCP) is a Senior Security Consultant at offensive cybersecurity firm Bishop Fox, where he specializes in red teaming, network penetration testing, and physical penetration testing. As a red team operator, he is adept at identifying critical attack chains that an external attacker could use to fully compromise organizations and reach high-value targets. Brandon is also recognized as a deepfake expert, conducting speaking sessions and live demonstrations at several global security and technology conferences. His research focuses on the intersection of offensive cybersecurity and artificial intelligence.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

AI Village - Saturday - 10:00-17:59 PDT

Title: Cyber Mirage: Realtime Deepfake Demos

Tags: AI Village | Creator Event/Activity

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 2 603 (AI Village) - [Map](#)

Description:

Go deepfake yourself! This hands-on demo shows how threat actors leverage open-source deepfake video and voice cloning frameworks to impersonate anyone in realtime, conducting social engineering and compromising organizations using nothing more than a consumer-grade gaming laptop. No specialized hardware, no budget, no nation-state resources required. Come learn the tradecraft firsthand and find out just how convincing you can become.

SpeakerBio: Brandon Kovacs

Brandon Kovacs (CRT, OSCP) is a Senior Security Consultant at offensive cybersecurity firm Bishop Fox, where he specializes in red teaming, network penetration testing, and physical penetration testing. As a red team operator, he is adept at identifying critical attack chains that an external attacker could use to fully compromise organizations and reach high-value targets. Brandon is also recognized as a deepfake expert, conducting speaking sessions and live demonstrations at several global security and technology conferences. His research focuses on the intersection of offensive cybersecurity and artificial intelligence.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Cyber Threat Intelligence 101: From Foundations to AI-Driven Defense

Tags: Blue Team Village | Creator Talk/Panel

When: Friday, Aug 7, 11:00 - 11:59 PDT

Where: LVCCW Level 2 W217 (Blue Team Village) Main Stage - [Map](#)

Description:

This talk is a fast-paced, vendor-neutral primer for defenders who want to turn raw telemetry into actionable intelligence. Threat intelligence is not just a feed — it is a discipline built through practice, structure, and action. This session introduces the CTI lifecycle, intelligence requirements, MITRE ATT&CK mapping, and the role of baselining in helping analysts separate normal activity from suspicious behavior.

Attendees will also see how CTI becomes operational through practical blue-team workflows such as YARA and Sigma rule development, threat hunting, incident response, and purple-team validation. We will close by exploring how grounded AI workflows can accelerate enrichment, ATT&CK mapping, detection drafting, and analyst reporting while keeping humans responsible for validation, context, and final decisions.

SpeakerBio: Carlo Anez Mazurco

Carlo Anez Mazurco is a cybersecurity instructor, consultant, and community leader with more than 15 years of experience across security operations, threat intelligence, incident response, threat hunting, and detection engineering. He is the Founder of IgniteCyber Academy, a DEF CON Training instructor, and an active contributor to Blue Team Village, where he supports Project Obsidian and develops hands-on blue team content for the cybersecurity community.

Carlo specializes in helping defenders translate attacker tradecraft into practical detection and response techniques while responsibly integrating artificial intelligence into modern security operations. His work focuses on creating realistic labs, CTF challenges, and immersive training environments that prepare students for real-world investigations using enterprise telemetry, cloud technologies, and AI-assisted workflows.

He has delivered training and presentations for conferences, universities, government organizations, and commercial teams, with a passion for mentoring the next generation of cybersecurity professionals. His goal is to make complex security concepts approachable through practical demonstrations, collaborative learning, and hands-on exercises that participants can immediately apply in their own environments.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Maker's Village - Friday - 15:00-16:59 PDT

Title: Cyberdeck Build

Tags: Maker's Village | Creator Event/Activity | Cyber Deck Makers' Contest

When: Friday, Aug 7, 15:00 - 16:59 PDT

Where: LVCCW Level 1 Hall 1 301 (Makers' Village) - [Map](#)

Description:

Learn some in's and out's of building your own cyberdeck... by building one with us! Customizable with radio add on, this deck is a great introduction level or intermediate refresher.

SpeakerBio: Sk!tz0

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Maker's Village - Saturday - 15:00-16:59 PDT

Title: Cyberdeck Build

Tags: Maker's Village | Creator Event/Activity | Cyber Deck Makers' Contest

When: Saturday, Aug 8, 15:00 - 16:59 PDT

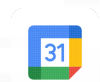
Where: LVCCW Level 1 Hall 1 301 (Makers' Village) - [Map](#)

Description:

Learn some in's and out's of building your own cyberdeck... by building one with us! Customizable with radio add on, this deck is a great introduction level or intermediate refresher.

SpeakerBio: Sk!tz0

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: CyberKB: When Your AI Copilot Runs the Recon, Crawls the Dark Web, and Maps the Kill Chain

Tags: Recon Village | Creator Talk/Panel

When: Saturday, Aug 8, 17:00 - 17:30 PDT

Where: LVCCW Level 1 Hall 3 801 (Creator Stage 2) - [Map](#)

Description:

What if your recon tool could understand "find leaked credentials for this company on the dark web, cross-reference with their exposed infrastructure, and show me the attack path" — and then actually do it, autonomously, with zero manual commands? CyberKB is a 214,000-line open platform that puts an AI copilot (Keke) in command of 131 offensive tools spanning reconnaissance, dark web OSINT, Shodan intelligence, breach databases, and a full Kali Linux shell — all orchestrated through natural language conversation. The Dark Web Intelligence Pipeline (DarkMonitor): CyberKB's DarkMonitor module queries .onion search engines concurrently through Tor, uses LLM-powered query refinement to generate optimal dark web search terms, applies AI relevance filtering to surface the most critical results.

The AI Copilot (Keke): Keke isn't a wrapper around ChatGPT. It's a function-calling agent with direct execution access to: a privileged Kali container (nmap, curl, nikto, sqlmap, gobuster, hydra — the full toolkit), 16 dark web search engines via Tor, breach and paste database aggregators, a RAG-powered knowledge base with semantic search over ingested recon data, Shodan lookups and CVE correlation, MITRE ATT&CK technique mapping, attack graph generation and path prioritization, and engagement management (targets, credentials, findings, reports).

Scale Proof — 2,250-Domain Assessment: We demonstrate CyberKB against a real-world external attack surface assessment: 2,250 domains belonging to a single organization, producing 11,968 unique IPs, 8,494 hostnames, 2,444 CVEs, 80,238 open ports, and a knowledge graph of 6,390 nodes with 51,990 infrastructure relationship edges. The entire dataset was parsed, correlated, and ingested into the AI-queryable knowledge base in 25 seconds. Keke can now answer questions like "which x domains share infrastructure with known-vulnerable IPs" by searching the graph, not by re-scanning.

What This Means for Defenders: Every autonomous recon step Keke performs leaves detectable artifacts. We discuss what blue teams should monitor: DNS burst patterns from multi-engine enumeration, Tor exit node correlation with target infrastructure, behavioral signatures of AI-driven sequential probing, and how to distinguish human recon from autonomous agent recon. The same platform that empowers red teams reveals the detection surface that defenders can leverage.

Key Takeaways: 1. AI copilots with direct tool execution compress hours of reconnaissance into minutes of conversation — fundamentally changing the operator's role from command executor to strategic decision-maker. 2. Dark web OSINT can be systematically automated with LLM-driven search refinement and relevance filtering, making it accessible beyond specialized analysts. 3. Infrastructure-scale attack surface mapping (2,250+ domains) becomes practical when AI handles correlation instead of humans. 4. Autonomous recon creates detectable patterns that blue teams should be actively hunting for. Tool Stack: Python, Flask, ChromaDB (RAG), Docker (Kali + Tor + Browser Agent), OpenAI-compatible LLM API, SQLite, Playwright, BeautifulSoup. 105 Python modules. Fully self-hosted — no cloud dependencies for core functionality.

Speakers: Suriya Prasath S, Chandru J, Muthu Kumar

SpeakerBio: Suriya Prasath S, zoho, red teamer, manager

A Red Teamer and Security Manager at Zoho CRM—Red Team, with 6+ years of experience driving adversarial simulations and real-world attack emulation at scale. He focuses on uncovering critical security gaps by thinking like an attacker—blending deep technical expertise with practical red team operations to challenge assumptions and strengthen defences.

SpeakerBio: Chandru J, Zoho, Product Security Manager

Product Security Manager with over 12 years of experience in driving cybersecurity initiatives, enhancing organizational security posture, and ensuring compliance with international standards such as ISO 27001, SOC 2, and GDPR. Adept at leading and mentoring teams, managing enterprise-wide security programs, and developing in-house security tools to address vulnerabilities effectively. Proven expertise in vulnerability management, incident response, security governance, and implementing secure development lifecycle (SDLC) practices. Recognized for fostering a security-first culture and collaborating with cross-functional teams to mitigate risks, protect assets, and improve processes in rapidly evolving environments.

SpeakerBio: Muthu Kumar, Security Engineer

I am a Security Engineer with 10 years of experience specializing in web application security and security tool development. I have extensive experience identifying security vulnerabilities, improving secure development practices, and building tools that help organizations detect and prevent security risks at scale.

My expertise includes application security testing, secure code reviews, threat modeling, vulnerability assessment, and developing security automation solutions that reduce manual effort and improve detection accuracy. I have worked on enhancing security tools by reducing false positives and helping engineering teams address vulnerabilities more efficiently.

I am passionate about building secure systems and solving complex security challenges through automation, innovation, and practical security engineering approaches. My focus is on strengthening application security while enabling development teams to build and ship secure products faster.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Damn Vulnerable Agentic AI Application (DVAIA)

Tags: Intro/Beginner | AI | DEF CON Demo Labs | AppSec | Offense/Red Team | DEF CON Demo Labs

When: Friday, Aug 7, 12:00 - 12:45 PDT

Where: LVCCW Level 1 Hall 3 1001 (Demo Labs Track 1) - [Map](#)

Description:

AI-powered Agentic applications now execute database queries, read files, send emails, and call APIs on behalf of users — all triggered through a chat window. DVAIA (Damn Vulnerable Agentic AI Application) is a new open-source platform purpose-built to let you break them.

DVAIA pairs a production-grade secure platform with deliberately vulnerable AI-powered chat agents, each isolated in its own database and mapped to the OWASP Top 10 for LLM Applications 2025. In this demo we live-exploit nine exercise categories covering 93 attack objectives:

- Prompt injection: extract system prompts, jailbreak filters, poison RAG documents, and hijack an email-summarization agent
- SQL and NoSQL injection through AI: trick chat agents into constructing malicious queries — the injection never touches a traditional input field
- Sensitive info disclosure: chain path traversal and SSRF through a banking agent's tool interface to read server secrets and probe internal services
- Excessive agency and BOLA: make a customer-service agent access other users' data, create unauthorized orders, and issue fraudulent refunds
- XSS and CSRF through LLM output: reflected, stored, and LLM-generated cross-site scripting fired from chat responses
- Supply chain RCE: exploit a poisoned dependency through conversation with a code-analysis agent

Speakers: Abhinav Verma, Mukesh Aggarwal

SpeakerBio: Abhinav Verma

Abhinav Verma is a Senior Staff Security Engineer at Intuit Inc. with 15+ years of experience across AI security, offensive security, red teaming, product security, and security operations. He currently leads AI security architecture reviews, AI penetration testing, and vulnerability management programs, with a focus on AI security, AI threat modeling, and securing large-scale cloud platforms.

Over the course of his career at Intuit, he has built security automation, scaled continuous security scanning across thousands of assets, led secure design reviews for platforms serving millions of customers, and developed secure coding programs that have helped thousands of engineers shift security left. Abhinav was formerly an independent security researcher and has identified and reported vulnerabilities in numerous major online services and technology companies.

He holds certifications including OSEP, OSCP, OSWP, GWAPT and CEH. Outside of work, Abhinav is a passionate gamer, a trained chef, an avid camper, and a mentor to aspiring offensive security practitioners.

SpeakerBio: Mukesh Aggarwal

Mukesh Aggarwal is a Distinguished Security Engineer who has spent his career thinking like a hacker. For nearly two decades he has hunted fraudsters and abuse across fintech platforms, building the detection pipelines, automations, and controls that shut bad actors down. He now lives at the bleeding edge of GenAI and agentic AI security, secure-by-default agent patterns, adversarial pen-testing and prompt-injection defense. He breaks things to understand them and stays a step

ahead of attackers, usually spotting the weaknesses before they do.

Mukesh has spoken at RSA Conference (OWASP GenAI Security Track), RenderATL, and the Intel Capital CISO Summit on AI safety, fraud, and offensive security, and is a member of the GIAC Advisory Board.

Off the clock he is a die-hard offensive-security tinkerer who reverse-engineers hardware and apps, pokes at IoT security, writes autonomous bots, and automates his home. He also mentors the next wave of offensive and AI security practitioners.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Damn Vulnerable Agentic AI Application (DVAIA)

Tags: Intro/Beginner | AI | DEF CON Demo Labs | AppSec | Offense/Red Team | DEF CON Demo Labs

When: Friday, Aug 7, 11:00 - 11:45 PDT

Where: LVCCW Level 1 Hall 3 1001 (Demo Labs Track 1) - [Map](#)

Description:

AI-powered Agentic applications now execute database queries, read files, send emails, and call APIs on behalf of users — all triggered through a chat window. DVAIA (Damn Vulnerable Agentic AI Application) is a new open-source platform purpose-built to let you break them.

DVAIA pairs a production-grade secure platform with deliberately vulnerable AI-powered chat agents, each isolated in its own database and mapped to the OWASP Top 10 for LLM Applications 2025. In this demo we live-exploit nine exercise categories covering 93 attack objectives:

- Prompt injection: extract system prompts, jailbreak filters, poison RAG documents, and hijack an email-summarization agent
- SQL and NoSQL injection through AI: trick chat agents into constructing malicious queries — the injection never touches a traditional input field
- Sensitive info disclosure: chain path traversal and SSRF through a banking agent's tool interface to read server secrets and probe internal services
- Excessive agency and BOLA: make a customer-service agent access other users' data, create unauthorized orders, and issue fraudulent refunds
- XSS and CSRF through LLM output: reflected, stored, and LLM-generated cross-site scripting fired from chat responses
- Supply chain RCE: exploit a poisoned dependency through conversation with a code-analysis agent

Speakers: Abhinav Verma, Mukesh Aggarwal

SpeakerBio: Abhinav Verma

Abhinav Verma is a Senior Staff Security Engineer at Intuit Inc. with 15+ years of experience across AI security, offensive security, red teaming, product security, and security operations. He currently leads AI security architecture reviews, AI penetration testing, and vulnerability management programs, with a focus on AI security, AI threat modeling, and securing large-scale cloud platforms.

Over the course of his career at Intuit, he has built security automation, scaled continuous security scanning across thousands of assets, led secure design reviews for platforms serving millions of customers, and developed secure coding programs that have helped thousands of engineers shift security left. Abhinav was formerly an independent security researcher and has identified and reported vulnerabilities in numerous major online services and technology companies.

He holds certifications including OSEP, OSCP, OSWP, GWAPT and CEH. Outside of work, Abhinav is a passionate gamer, a trained chef, an avid camper, and a mentor to aspiring offensive security practitioners.

SpeakerBio: Mukesh Aggarwal

Mukesh Aggarwal is a Distinguished Security Engineer who has spent his career thinking like a hacker. For nearly two decades he has hunted fraudsters and abuse across fintech platforms, building the detection pipelines, automations, and controls that shut bad actors down. He now lives at the bleeding edge of GenAI and agentic AI security, secure-by-default agent patterns, adversarial pen-testing and prompt-injection defense. He breaks things to understand them and stays a step

ahead of attackers, usually spotting the weaknesses before they do.

Mukesh has spoken at RSA Conference (OWASP GenAI Security Track), RenderATL, and the Intel Capital CISO Summit on AI safety, fraud, and offensive security, and is a member of the GIAC Advisory Board.

Off the clock he is a die-hard offensive-security tinkerer who reverse-engineers hardware and apps, pokes at IoT security, writes autonomous bots, and automates his home. He also mentors the next wave of offensive and AI security practitioners.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

DEF CON Training - Monday - 08:30-17:30 PDT

Title: Dark Wolf Hack Our Drone Workshop

Tags: DEF CON Training (Paid) (2-day) | DEF CON Training

When: Monday, Aug 10, 08:30 - 17:30 PDT

Where:

Description:

Speakers:Ronald Broberg,Rudy Mendoza

SpeakerBio: Ronald Broberg

No BIO available

SpeakerBio: Rudy Mendoza

No BIO available

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

DEF CON Training - Tuesday - 08:30-17:30 PDT

Title: Dark Wolf Hack Our Drone Workshop

Tags: DEF CON Training (Paid) (2-day) | DEF CON Training

When: Tuesday, Aug 11, 08:30 - 17:30 PDT

Where:

Description:

Speakers:Ronald Broberg,Rudy Mendoza

SpeakerBio: Ronald Broberg

No BIO available

SpeakerBio: Rudy Mendoza

No BIO available

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

DEF CON Groups - Friday - 13:30-14:30 PDT

Title: Darknet Diaries Meet & Greet with Jack Rhysider

Tags: DEF CON Groups | Creator Event/Activity

When: Friday, Aug 7, 13:30 - 14:30 PDT

Where: LVCCW Level 2 W238 (DEF CON Groups) - [Map](#)

Description:

Meet Jack Rhysider, creator and host of Darknet Diaries, during a special fan meet and greet in the DEF CON Groups Community. Stop by to say hello and talk about your favorite stories from the dark side of the internet. First come, first served.

SpeakerBio: Jack Rhysider, Creator and Host at Darknet Diaries

No BIO available

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Contests - Friday - 10:00-17:59 PDT

Title: Darknet-NG

Tags: Darknet-NG | Contest

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 105 (Darknet-NG) - [Map](#)

Description:

Darknet-NG is an Alternate Reality Game (ARG), where the players take on the Persona of an Agent who is sent on Quests to learn real skills and gain in-game points. If this is your first time at DEF CON, this is a great place to start, because we assume no prior knowledge. Building from basic concepts, we teach agents about a range of topics from Lock-picking, to using and decoding ciphers, to Electronics 101, just to name a few, all while also helping to connect them to the larger DEF CON Community. The "Learning Quests" help the agent gather knowledge from all across the other villages at the conference, while the "Challenge Quests" help hone their skills! Sunday Morning there is a BOSS FIGHT where the Agents must use their combined skills as a community and take on that year's final challenge! There is a whole skill tree of personal knowledge to obtain, community to connect with and memories to make! To get started, check out our site <https://darknet-ng.network> and join our growing Community!

Participant Prerequisites

Prerequisites for competing in the contest would require a device with access to a web browser like a Phone, Tablet, Laptop.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Contests - Saturday - 10:00-17:59 PDT

Title: Darknet-NG

Tags: Darknet-NG | Contest

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 105 (Darknet-NG) - [Map](#)

Description:

Darknet-NG is an Alternate Reality Game (ARG), where the players take on the Persona of an Agent who is sent on Quests to learn real skills and gain in-game points. If this is your first time at DEF CON, this is a great place to start, because we assume no prior knowledge. Building from basic concepts, we teach agents about a range of topics from Lock-picking, to using and decoding ciphers, to Electronics 101, just to name a few, all while also helping to connect them to the larger DEF CON Community. The "Learning Quests" help the agent gather knowledge from all across the other villages at the conference, while the "Challenge Quests" help hone their skills! Sunday Morning there is a BOSS FIGHT where the Agents must use their combined skills as a community and take on that year's final challenge! There is a whole skill tree of personal knowledge to obtain, community to connect with and memories to make! To get started, check out our site <https://darknet-ng.network> and join our growing Community!

Participant Prerequisites

Prerequisites for competing in the contest would require a device with access to a web browser like a Phone, Tablet, Laptop.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Contests - Sunday - 10:00-11:59 PDT

Title: Darknet-NG

Tags: Darknet-NG | Contest

When: Sunday, Aug 9, 10:00 - 11:59 PDT

Where: LVCCW Level 1 Hall 1 105 (Darknet-NG) - [Map](#)

Description:

Darknet-NG is an Alternate Reality Game (ARG), where the players take on the Persona of an Agent who is sent on Quests to learn real skills and gain in-game points. If this is your first time at DEF CON, this is a great place to start, because we assume no prior knowledge. Building from basic concepts, we teach agents about a range of topics from Lock-picking, to using and decoding ciphers, to Electronics 101, just to name a few, all while also helping to connect them to the larger DEF CON Community. The "Learning Quests" help the agent gather knowledge from all across the other villages at the conference, while the "Challenge Quests" help hone their skills! Sunday Morning there is a BOSS FIGHT where the Agents must use their combined skills as a community and take on that year's final challenge! There is a whole skill tree of personal knowledge to obtain, community to connect with and memories to make! To get started, check out our site <https://darknet-ng.network> and join our growing Community!

Participant Prerequisites

Prerequisites for competing in the contest would require a device with access to a web browser like a Phone, Tablet, Laptop.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: DarkSyringe: Automated poisoning of Clinical AI Assistants Through PDFs (a physician's point of view)

Tags: Biohacking Village | Creator Talk/Panel

When: Saturday, Aug 8, 15:30 - 15:59 PDT

Where: LVCCW Level 1 Hall 3 1104 (Creator Stage 4) - [Map](#)

Description:

Doctors are burned out and turning to LLMs — uploading discharge letters, lab reports and papers into ChatGPT, Claude and clinical AI tools. Every PDF is an unvalidated input to a system that cannot tell real facts from injected lies. We introduce Divergent Prompt Injection: unlike classic attacks ("ignore previous instructions"), divergent payloads are clinically plausible false statements — a wrong drug, a fabricated contraindication, a phantom diagnosis — embedded in medical content. They create no semantic conflict, trigger no detection system, and sit indistinguishable from real medicine until an LLM summarizes them into a treatment plan.

We release DarkSyringe, an open-source tool automating the full attack chain: PDF ingestion, de-identification, LLM-driven payload generation, injection and multi-model scoring. In testing, a single poisoned discharge letter caused multiple commercial LLMs to recommend wrong drugs, fabricate contraindications and invent diagnoses — errors that would directly harm patients.

This talk brings a physician's perspective: understanding why even a low-complexity attack becomes critical when it lands in a clinical environment built on time pressure, trust, and information overload.

SpeakerBio: Francesco Costa

Hand surgeon trainee and cybersecurity researcher focused on LLM security. Creator of DarkSyringe, combining real clinical experience with offensive research to expose the limits of current defenses.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

The Diana Initiative - Saturday - 10:30-10:40 PDT

Title: Data Duplication Village Tour

Tags: The Diana Initiative | Creator Tour

When: Saturday, Aug 8, 10:30 - 10:40 PDT

Where: LVCCW Level 1 South Lobby / Atrium - [Map](#)

Description:

Interested in visiting Data Duplication Village but afraid to go by yourself? The Diana Initiative is hosting tours! Follow a volunteer to Data Duplication Village and be introduced to the community and activities inside!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Data Tomb Raider: Raiding Modern AI Vaults with Legacy Flaws for Treasure Stealing

Tags: DEF CON Official Talk | Demo | Exploit

When: Friday, Aug 7, 15:00 - 15:59 PDT

Where: LVCCW Level 1 Hall 3 906 (Main Track 3) - [Map](#)

Description:

Click a link, lose your MFA codes. Your AI assistant reads your email and exfiltrates the data through Bing, and you never notice.

We found a 1-click attack chain against Microsoft 365 Copilot that combines three vulnerability classes everyone assumed were solved - CSP, SSRF, and HTML injection - into one kill shot. A URL parameter lands directly in the AI engine as an executable prompt, a vector we call Parameter-to-Prompt (P2P) injection. The AI searches the victim's mailbox, grabs sensitive data, and emits an img tag with the loot in the URL. That tag renders mid-stream, before the output sanitizer fires, because sanitization is a post-processing step. The img src hits Bing's Search by Image endpoint - CSP-allowlisted - which server-side fetches to our domain, tunneling stolen data through Microsoft's own infrastructure.

CSP enforced. Sanitizer running. AI guardrails active. All three defenses in place - the chain walked right through them. None of these bugs are new. Each has textbook mitigations. But nobody tests what happens when old web bugs compose with AI behaviors - web teams and AI teams don't test each other's seams. We break down the full chain, demo it live, and hand you a methodology for hunting composition bugs across AI-integrated platforms.

Speakers: Dolev Taler, Mark Vaitsman

SpeakerBio: Dolev Taler, Varonis

Dolev Taler is a senior security researcher at Varonis Threat Labs with over a decade of cybersecurity experience spanning red teaming, reverse engineering, vulnerability research, and malware analysis. He is passionate about machine learning and its pivotal role in modern threat detection, having developed advanced detection models, investigated ransomware attacks for major global enterprises, and reported vulnerabilities in critical infrastructure systems. Beyond tackling high-stakes cyber threats, Dolev also enjoys perfecting the art of coffee brewing and improving his lock-picking skills.

SpeakerBio: Mark Vaitsman, Varonis

Mark Vaitsman is a Security Research Team Leader at Varonis, a leader in Data Security. He is a passionate cybersecurity expert with extensive experience in leading security threat and research teams in various Cyber Security companies, analyzing emerging threats, incident response and developing innovative solutions. Mark is also a lecturer of Cyber Security courses, sharing his knowledge and shaping the next generation of cybersecurity professionals. Previously spoken at BlackHat, DeepSec, RSAC, CrestCon. In his free time he likes sailing in the sea and riding a motorcycle.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Noob Community - Friday - 14:15-14:45 PDT

Title: Day in the Life - Green Beret to AI Penetration Tester

Tags: Noob Community | Creator Talk/Panel

When: Friday, Aug 7, 14:15 - 14:45 PDT

Where: LVCCW Level 1 Hall 4 1417 (Noob Community) - [Map](#)

Description:

This session is an open on building a career in offensive security, from unconventional beginnings to breaking AI systems at a major tech company.

The speaker will share a candid look at his journey from U.S. Army Special Forces to national-level cyber operations and now AI penetration testing highlighting what actually mattered, what didn't, and how skills from completely different fields translate into high-end offensive security roles.

Topics will range from breaking into cybersecurity with no experience, navigating certifications and degrees, and building real-world skills through CTFs and labs to what it's like to hack AI systems, how those attacks work in practice, and where the field is heading.

SpeakerBio: Clayton Boozell

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Social Gatherings/Events - Friday - 21:00-00:59 PDT

Title: Day of the Dead Hacker Party

Tags: Party

When: Friday, Aug 7, 21:00 - 00:59 PDT

Where: LVCCW Level 3 W327 (Misc Meeting Room) - [Map](#)

Description:

Join us as we celebrate the lives, legends, and lasting influence of the hackers who shaped our world. From pioneers of the underground to cultural icons of the digital frontier whose stories still echo through the system.

Dress in Day of the Dead attire or come as a ghost of hacker culture, dead heroes, legendary coders, digital outlaws, and spirits of the machine.

Music by CURZE\$ and special guest DJs.

Everyone is welcome to join us and celebrate the dead, the code, and the culture that refuses to die.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

The Diana Initiative - Friday - 12:10-12:20 PDT

Title: DC Maker's Community Tour

Tags: The Diana Initiative | Creator Tour

When: Friday, Aug 7, 12:10 - 12:20 PDT

Where: LVCCW Level 1 South Lobby / Atrium - [Map](#)

Description:

Interested in visiting DC Maker's Community but afraid to go by yourself? The Diana Initiative is hosting tours! Follow a volunteer to DC Maker's Community and be introduced to the community and activities inside!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Contests - Saturday - 10:00-17:59 PDT

Title: DC's Next Top Threat Model

Tags: DC's Next Top Threat Model | Contest

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 102 (DC's Next Top Threat Model) - [Map](#)

Description:

Threat Modeling is arguably the single most important activity in an application security program and if performed early can identify a wide range of potential flaws before a single line of code has been written. While being so critically important there is no single correct way to perform Threat Modeling, many techniques, methodologies and/or tools exist.

As part of our challenge we will present contestants with the exact same design and compare the outputs they produce against a number of categories in order to identify a winner and crown DEF CON's Next Top Threat Model(er).

Participant Prerequisites

A laptop is recommended, a smartphone could be used but will be less than ideal. Internet access to retrieve the design materials and to submit findings and access to the email used during registration.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Contests - Friday - 10:00-17:59 PDT

Title: DC's Next Top Threat Model

Tags: DC's Next Top Threat Model | Contest

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 102 (DC's Next Top Threat Model) - [Map](#)

Description:

Threat Modeling is arguably the single most important activity in an application security program and if performed early can identify a wide range of potential flaws before a single line of code has been written. While being so critically important there is no single correct way to perform Threat Modeling, many techniques, methodologies and/or tools exist.

As part of our challenge we will present contestants with the exact same design and compare the outputs they produce against a number of categories in order to identify a winner and crown DEF CON's Next Top Threat Model(er).

Participant Prerequisites

A laptop is recommended, a smartphone could be used but will be less than ideal. Internet access to retrieve the design materials and to submit findings and access to the email used during registration.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Contests - Sunday - 10:00-11:59 PDT

Title: DC's Next Top Threat Model

Tags: DC's Next Top Threat Model | Contest

When: Sunday, Aug 9, 10:00 - 11:59 PDT

Where: LVCCW Level 1 Hall 1 102 (DC's Next Top Threat Model) - [Map](#)

Description:

Threat Modeling is arguably the single most important activity in an application security program and if performed early can identify a wide range of potential flaws before a single line of code has been written. While being so critically important there is no single correct way to perform Threat Modeling, many techniques, methodologies and/or tools exist.

As part of our challenge we will present contestants with the exact same design and compare the outputs they produce against a number of categories in order to identify a winner and crown DEF CON's Next Top Threat Model(er).

Participant Prerequisites

A laptop is recommended, a smartphone could be used but will be less than ideal. Internet access to retrieve the design materials and to submit findings and access to the email used during registration.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: DC101

Tags: DEF CON Official Talk

When: Friday, Aug 7, 12:30 - 12:59 PDT

Where: LVCCW Level 1 Hall 3 801 (Creator Stage 1) - [Map](#)

Description:

Speakers: Nikita Kronenberg, Michael “sparky” Moore, polybius

SpeakerBio: Nikita Kronenberg

No BIO available

SpeakerBio: Michael “sparky” Moore, Lead, Network Operations Center at DEF CON

Michael Moore “sparky” somehow convinced people to let him run the DEF CON Network Operations Center, where he leads the team responsible for building and operating the network that thousands of attendees immediately try to break. With more than 20 years with DEF CON, project management, and technical leadership, he’s learned that every impossible deadline is just another networking problem with better marketing. He’s still waiting for the year everything works exactly as planned.

SpeakerBio: polybius, Global Village Lead at DEF CON Communications

^_(,)_/

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Social Gatherings/Events - Thursday - 19:00-21:59 PDT

Title: DC702 Meetup

Tags: Meetup

When: Thursday, Aug 6, 19:00 - 21:59 PDT

Where: LVCCW Level 3 W327 (Misc Meeting Room) - [Map](#)

Description:

Join the local DC702 Group in this year's official DEF CON Meetup! The meetup will be casual and include typical meetup activities (e.g., socializing, "challenges," lockpicking, music, etc.) and maybe a few little surprises.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Social Gatherings/Events - Wednesday - 18:30-21:30 PDT

Title: DC713 and DC281 - 8th Annual DEF CON Texas Groups Meetup

Tags: Meetup

When: Wednesday, Aug 5, 18:30 - 21:30 PDT

Where: Other / See Description

Description:

We are back hacker fam!

The Texas Crew welcomes all DEF CON friends to our 8th annual meetup.

Hosted by The Cornish Pasty

10 E Charleston Blvd, Las Vegas, NV 89104

Come for the friends. Stay for the pasties. See you there!

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Social Gatherings/Events - Saturday - 15:00-16:59 PDT

Title: DCG New England Meetup

Tags: Meetup

When: Saturday, Aug 8, 15:00 - 16:59 PDT

Where: LVCCW Level 3 W327 (Misc Meeting Room) - [Map](#)

Description:

New England's hackers are spread across six smaller states and rarely in the same room. This is the room. DCG New England pulls the region's groups and unaffiliated folks together to hang out, meet other hackers in the region, talk shop, show off half-finished projects, and meet the people who keep the local scene ticking.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Aerospace Village - Sunday - 10:00-13:59 PDT

Title: DCNextGen - Bricks in the Air

Tags: Aerospace Village | Creator Event/Activity

When: Sunday, Aug 9, 10:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 2 700 (Aerospace Village) - [Map](#)

Description:

Step right up to our interactive LEGO aircraft. Can you investigate the aircraft's control system, identify any vulnerabilities, and “hack” beyond its intended functions?

This exercise uses real-world I2C protocols to simulate potential vulnerabilities in an aircraft control system.

No specialized hardware required - all target devices, materials, and interfaces are provided!

No prior aviation or security experience required - a walkthrough guide is provided for beginners, and volunteers are on hand to help at every step. This activity is accessible to all skill levels.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Aerospace Village - Saturday - 10:00-17:59 PDT

Title: DCNextGen - Bricks in the Air

Tags: Aerospace Village | Creator Event/Activity

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 2 700 (Aerospace Village) - [Map](#)

Description:

Step right up to our interactive LEGO aircraft. Can you investigate the aircraft's control system, identify any vulnerabilities, and “hack” beyond its intended functions?

This exercise uses real-world I2C protocols to simulate potential vulnerabilities in an aircraft control system.

No specialized hardware required - all target devices, materials, and interfaces are provided!

No prior aviation or security experience required - a walkthrough guide is provided for beginners, and volunteers are on hand to help at every step. This activity is accessible to all skill levels.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Aerospace Village - Friday - 10:00-17:59 PDT

Title: DCNextGen - Bricks in the Air

Tags: Aerospace Village | Creator Event/Activity

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 2 700 (Aerospace Village) - [Map](#)

Description:

Step right up to our interactive LEGO aircraft. Can you investigate the aircraft's control system, identify any vulnerabilities, and “hack” beyond its intended functions?

This exercise uses real-world I2C protocols to simulate potential vulnerabilities in an aircraft control system.

No specialized hardware required - all target devices, materials, and interfaces are provided!

No prior aviation or security experience required - a walkthrough guide is provided for beginners, and volunteers are on hand to help at every step. This activity is accessible to all skill levels.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Aerospace Village - Friday - 10:00-17:59 PDT

Title: DCNextGen - RIC-1: ELT Localization Exercise - N3VR-G0N Down

Tags: Aerospace Village | Creator Event/Activity

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 2 700 (Aerospace Village) - [Map](#)

Description:

RIC-1, tail number N3VR-G0N, has gone down! You need to use radio direction-finding (RDF) techniques to locate Emergency Locator Transmitter (ELT), report its position, and help rescue our missing pilot!

Participants will use the provided handheld DF equipment provided by the Village, or bring your own, to triangulate the hidden transmitter location within the village area. Your handheld radio must be capable of receiving on the designated frequency with a directional antenna or attenuator. Once you've located RIC-1, listen closely... you may recognize the beacon's "distress tone." It appears to be broadcasting an audio payload that responders have described as "oddly catchy" and "impossible to stop once you start listening." Bring your comfortable shoes and strong will to ensure you never give up until you find our missing pilot!

No prior RDF experience required - volunteers can walk you through basic triangulation techniques before you start this 15-30 minute event.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Aerospace Village - Sunday - 10:00-13:59 PDT

Title: DCNextGen - RIC-1: ELT Localization Exercise - N3VR-G0N Down

Tags: Aerospace Village | Creator Event/Activity

When: Sunday, Aug 9, 10:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 2 700 (Aerospace Village) - [Map](#)

Description:

RIC-1, tail number N3VR-G0N, has gone down! You need to use radio direction-finding (RDF) techniques to locate Emergency Locator Transmitter (ELT), report its position, and help rescue our missing pilot!

Participants will use the provided handheld DF equipment provided by the Village, or bring your own, to triangulate the hidden transmitter location within the village area. Your handheld radio must be capable of receiving on the designated frequency with a directional antenna or attenuator. Once you've located RIC-1, listen closely... you may recognize the beacon's "distress tone." It appears to be broadcasting an audio payload that responders have described as "oddly catchy" and "impossible to stop once you start listening." Bring your comfortable shoes and strong will to ensure you never give up until you find our missing pilot!

No prior RDF experience required - volunteers can walk you through basic triangulation techniques before you start this 15-30 minute event.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Aerospace Village - Saturday - 10:00-17:59 PDT

Title: DCNextGen - RIC-1: ELT Localization Exercise - N3VR-G0N Down

Tags: Aerospace Village | Creator Event/Activity

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 2 700 (Aerospace Village) - [Map](#)

Description:

RIC-1, tail number N3VR-G0N, has gone down! You need to use radio direction-finding (RDF) techniques to locate Emergency Locator Transmitter (ELT), report its position, and help rescue our missing pilot!

Participants will use the provided handheld DF equipment provided by the Village, or bring your own, to triangulate the hidden transmitter location within the village area. Your handheld radio must be capable of receiving on the designated frequency with a directional antenna or attenuator. Once you've located RIC-1, listen closely... you may recognize the beacon's "distress tone." It appears to be broadcasting an audio payload that responders have described as "oddly catchy" and "impossible to stop once you start listening." Bring your comfortable shoes and strong will to ensure you never give up until you find our missing pilot!

No prior RDF experience required - volunteers can walk you through basic triangulation techniques before you start this 15-30 minute event.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Aerospace Village - Friday - 10:00-17:59 PDT

Title: DCNextGen - Space Grand Challenge - SatHack: The MOUSE-1 Mission

Tags: Aerospace Village | Creator Event/Activity

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 2 700 (Aerospace Village) - [Map](#)

Description:

The MOUSE-1 satellite is currently in Safe Mode, and its attitude and heading systems are behaving unexpectedly. Ground control needs answers NOW!

You are a newly assigned Mission Specialist, and it's your job to figure out what's going on. Work through five sequential challenge missions aboard a simulated HUD - complete with live orbital tracking, optical camera feeds, and attitude telemetry - to triage MOUSE-1, uncover what happened, and make it operational again.

Participants will learn how satellites operate, how they stay secure in orbit, and what happens when they don't - using a fully browser-based, gamified interface developed by California Polytechnic State University students.

Just grab a seat in front of the provided station, no prior cybersecurity or aerospace experience required! Each mission is self-guided with built-in instructions, and volunteers are available to assist. Both beginner and experienced participants will find this 30-minute event challenging and fun.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Aerospace Village - Saturday - 10:00-17:59 PDT

Title: DCNextGen - Space Grand Challenge - SatHack: The MOUSE-1 Mission

Tags: Aerospace Village | Creator Event/Activity

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 2 700 (Aerospace Village) - [Map](#)

Description:

The MOUSE-1 satellite is currently in Safe Mode, and its attitude and heading systems are behaving unexpectedly. Ground control needs answers NOW!

You are a newly assigned Mission Specialist, and it's your job to figure out what's going on. Work through five sequential challenge missions aboard a simulated HUD - complete with live orbital tracking, optical camera feeds, and attitude telemetry - to triage MOUSE-1, uncover what happened, and make it operational again.

Participants will learn how satellites operate, how they stay secure in orbit, and what happens when they don't - using a fully browser-based, gamified interface developed by California Polytechnic State University students.

Just grab a seat in front of the provided station, no prior cybersecurity or aerospace experience required! Each mission is self-guided with built-in instructions, and volunteers are available to assist. Both beginner and experienced participants will find this 30-minute event challenging and fun.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Aerospace Village - Sunday - 10:00-13:59 PDT

Title: DCNextGen - Space Grand Challenge - SatHack: The MOUSE-1 Mission

Tags: Aerospace Village | Creator Event/Activity

When: Sunday, Aug 9, 10:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 2 700 (Aerospace Village) - [Map](#)

Description:

The MOUSE-1 satellite is currently in Safe Mode, and its attitude and heading systems are behaving unexpectedly. Ground control needs answers NOW!

You are a newly assigned Mission Specialist, and it's your job to figure out what's going on. Work through five sequential challenge missions aboard a simulated HUD - complete with live orbital tracking, optical camera feeds, and attitude telemetry - to triage MOUSE-1, uncover what happened, and make it operational again.

Participants will learn how satellites operate, how they stay secure in orbit, and what happens when they don't - using a fully browser-based, gamified interface developed by California Polytechnic State University students.

Just grab a seat in front of the provided station, no prior cybersecurity or aerospace experience required! Each mission is self-guided with built-in instructions, and volunteers are available to assist. Both beginner and experienced participants will find this 30-minute event challenging and fun.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: DCNextGen Closing Ceremonies

Tags: DCNextGen | Creator Talk/Panel | Youth

When: Sunday, Aug 9, 13:30 - 14:30 PDT

Where: LVCCW Level 3 W316 (DC NextGen) - [Map](#)

Description:

And just like that, it's a wrap! While we're sad to see the fun end, we want to give everyone one last big thank you.

Join us to say goodbye to new friends and hear about all the cool plans we have for next year. We'll also be handing out prizes for our DCNextGen Badge CTF — you must be present to win!

SpeakerBio: BiaSciLab

No BIO available

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

DCNextGen - Friday - 10:30-11:30 PDT

Title: DCNextGen Opening Ceremonies

Tags: DCNextGen | Creator Talk/Panel | Youth

When: Friday, Aug 7, 10:30 - 11:30 PDT

Where: LVCCW Level 3 W316 (DC NextGen) - [Map](#)

Description:

Come pick up your DCNextGen electronic badge and swag! Get a preview of all the upcoming activities and adventures. We'll also show you how to use your new badge in order to participate in all of our cool ctf challenges around the conference!

SpeakerBio: BiaSciLab

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Social Gatherings/Events - Saturday - 19:00-20:59 PDT

Title: DCNextGen Party!

Tags: Party | DCNextGen | Youth

When: Saturday, Aug 8, 19:00 - 20:59 PDT

Where: LVCCW Level 3 W316 (DC NextGen) - [Map](#)

Description:

Are you ready to rock? If so, come to the DCNextGen party where the theme is UV cyberpunk! What is there to do you might ask? We have games, music, create your own raccoon mask, glow in the dark tattoos, and so much more! There is no better place to make new friends and hang out with your fellow DCNextGen cyber warriors.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

The Diana Initiative - Friday - 12:50-12:59 PDT

Title: DDoS Community Tour

Tags: The Diana Initiative | Creator Tour

When: Friday, Aug 7, 12:50 - 12:59 PDT

Where: LVCCW Level 1 South Lobby / Atrium - [Map](#)

Description:

Interested in visiting DDoS Community but afraid to go by yourself? The Diana Initiative is hosting tours! Follow a volunteer to DDoS Community and be introduced to the community and activities inside!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Data Duplication Village - Friday - 10:00-17:59 PDT

Title: DDV open and accepting drives for duplication

Tags: Data Duplication Village | Creator Event/Activity

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 2 W203 (Data Duplication Village) - [Map](#)

Description:

We start taking drives at 4: 00pm local time on Thursday - possibly a little earlier. We'll keep accepting drives until we reach capacity (usually late Friday or early Saturday). Then we copy and copy all the things until we just can't copy any more - first come, first served. Note that some sources require 8TB drives now. We run around the clock until we run out of time on Sunday morning with the last possible pickup being before 11:00am on Sunday.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Data Duplication Village - Thursday - 16:00-18:59 PDT

Title: DDV open and accepting drives for duplication

Tags: Data Duplication Village | Creator Event/Activity

When: Thursday, Aug 6, 16:00 - 18:59 PDT

Where: LVCCW Level 2 W203 (Data Duplication Village) - [Map](#)

Description:

We start taking drives at 4: 00pm local time on Thursday - possibly a little earlier. We'll keep accepting drives until we reach capacity (usually late Friday or early Saturday). Then we copy and copy all the things until we just can't copy any more - first come, first served. Note that some sources require 8TB drives now. We run around the clock until we run out of time on Sunday morning with the last possible pickup being before 11:00am on Sunday.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Data Duplication Village - Saturday - 10:00-17:59 PDT

Title: DDV open and accepting drives for duplication

Tags: Data Duplication Village | Creator Event/Activity

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 2 W203 (Data Duplication Village) - [Map](#)

Description:

We start taking drives at 4: 00pm local time on Thursday - possibly a little earlier. We'll keep accepting drives until we reach capacity (usually late Friday or early Saturday). Then we copy and copy all the things until we just can't copy any more - first come, first served. Note that some sources require 8TB drives now. We run around the clock until we run out of time on Sunday morning with the last possible pickup being before 11:00am on Sunday.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: De la Explotación de Buffer Overflows al C2 Industrial: Infectando y Controlando RTUs con Malware

Tags: La Villa Community | Creator Talk/Panel

When: Saturday, Aug 8, 16:30 - 17:30 PDT

Where: LVCCW Level 1 Hall 4 1416 (La Villa Community) Main Stage - [Map](#)

Description:

En esta charla práctica y directa al punto, se demostrará cómo una vulnerabilidad de buffer overflow puede ser explotada para comprometer entornos SCADA, evolucionando desde la ejecución de shellcode multietapa hasta el establecimiento de canales de comunicación C2 y el control remoto de sistemas industriales críticos. A través de demostraciones técnicas, se analizará cómo una vulnerabilidad aparentemente aislada puede convertirse en una cadena de ataque capaz de afectar procesos industriales, provocar interrupciones operativas e incluso derivar en escenarios de blackout.

SpeakerBio: Fernando Mengali, Information Security Specialist

Cybersecurity researcher focused on Pentesting and AppSec, also serving as a Practical / Hands-on Speaker. He also dedicates part of his research to critical infrastructure security (ICS/SCADA), exploring the intersection between classic vulnerabilities and industrial environments. He has over 18 years of experience in offensive security and practical application exploitation.

He has participated in research and development projects focused on vulnerability exploitation and offensive security.

Specialized in 0day discovery and exploit development, he has over 135 published CVEs and is ranked in the Top 10 contributors on VulDB <https://vuldb.com/users.top>.

Additionally, he has published multiple exploits and technical papers publicly available <https://www.exploit-db.com/?author=12136> and <https://packetstorm.news/files/author/8470/1>.

His work focuses on real-world vulnerability exploitation, including advanced scenarios such as memory corruption, buffer overflows, and complex environments.

He is the creator of <https://yrprey.com>, an educational framework that brings together more than 20 vulnerable applications based on the OWASP Top 10, used for practical training in Application Security and Offensive Security <https://owasp.org/www-project-vulnerable-web-application-directory>.

He is also the driving force behind <https://speakfy.io>, a project focused on promoting Information Security events globally.

Furthermore, he develops application security-oriented tools, such as <https://leapfix.co> (static code analysis) and <https://fitoxs.com>, a dynamic application analysis platform powered by artificial intelligence.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: De la nube a la corona: Uso indebido de la identidad híbrida en Azure DevOps Azure, AD, AWS y EKS

Tags: La Villa Community | Creator Workshop

When: Friday, Aug 7, 10:30 - 12:59 PDT

Where: LVCCW Level 1 Hall 4 1416 (La Villa Community) Workshops/Chillout - [Map](#)

Description:

Demostrar cómo las relaciones de confianza entre entornos híbridos de Azure DevOps, Microsoft Azure, Active Directory, Amazon Web Services y Kubernetes pueden ser abusadas por un atacante para realizar movimientos laterales, escalamiento de privilegios y compromiso de identidades utilizando herramientas y funcionalidades legítimas de administración cloud en infraestructuras híbridas corporativas.

Speakers: Juan Camilo Palacio Arango, Andrés Restrepo

SpeakerBio: Juan Camilo Palacio Arango, Un token, una confianza, una cadena de compromiso.

Juan Camilo Palacio

Suboficial retirado de la Fuerza Aérea Colombiana, con sólida formación en Ingeniería de Sistemas y un Máster en Ciberseguridad y Privacidad. A lo largo de los últimos 7 años, he perfeccionado y especializado mis habilidades en diversas áreas de la Ciberseguridad, Ciberdefensa y Ciberinteligencia, aplicando con éxito mis conocimientos en los sectores de defensa nacional y financiero.

Mi compromiso con la actualización constante de técnicas se evidencia en la obtención de certificaciones destacadas en técnicas de ethical hacking y red teaming, tales como OSEP, OSCP, CRTO, ARTE, CRTE, entre otras. Estas certificaciones expresan mi dedicación continua a la mejora de mis habilidades y destacan mi capacidad para enfrentar desafíos complejos en el dinámico campo de la ciberseguridad.

Andres Restrepo Gonzalez

Profesional de ciberseguridad especializado en Red Team y seguridad ofensiva en entornos multicloud. Cuenta con certificaciones avanzadas en AWS, Azure y operaciones de Red Team, incluyendo OSCP, CRTE, CRTP, CARTS, CCPenX-AWS y MCRTA, entre otras. Su trabajo se enfoca en la simulación de adversarios, pentesting de infraestructuras cloud y evaluación de la resiliencia de organizaciones frente a amenazas avanzadas.

SpeakerBio: Andrés Restrepo, Hacker

Entusiasta de la seguridad con experiencia en actividades de RedTeam

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Bug Bounty Village - Saturday - 11:30-12:30 PDT

Title: De-Sloppify: Your AI Needs a Proxy

Tags: Bug Bounty Village | Creator Workshop

When: Saturday, Aug 8, 11:30 - 12:30 PDT

Where: LVCCW Level 2 W206-207 (Bug Bounty Village) - [Map](#)

Description:

In the workshop we will explore how to setup yourself for success with AI agents by using a tight integration with your proxy of choice. We will start with why you would want to use a proxy with AI agents (Scoping, Guardrails, Human-in-the-loop, Tool provider) and then showcase multiple ways to achieve the integration (MCP, Skills, Plugins). It will use Caido for the workshop but the concepts will be applicable to all proxies.

Speakers:Emile "TheSydden" Fugulin,Vitor "busf4ctor" Falcao Habibe Costa

SpeakerBio: Emile "TheSydden" Fugulin, Caido Labs

Emile was a freelance devops & backend developer for many years prior to starting Caido. He always had a passion for security and working on Caido is the perfect combinaison of both!

SpeakerBio: Vitor "busf4ctor" Falcao Habibe Costa, Frontier AI Red Team Operator, BT6

Vitor is an AI security researcher, Community Manager at Critical Thinking, and a Google VRP hunter, named Best AI Researcher at Google bugSWAT. He's part of the BT6 team and hunts bugs full time.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

The Diana Initiative - Friday - 15:00-15:59 PDT

Title: Dear Red Team, Love Blue Team: Pulling Both Screaming Parties into Purple

Tags: The Diana Initiative | Creator Talk/Panel

When: Friday, Aug 7, 15:00 - 15:59 PDT

Where: LVCCW Level 2 W209 (Diana Initiative) - [Map](#)

Description:

While purple teaming isn't a new concept, getting purple teaming actually started and happening consistently is tough! Maybe your company or team experienced the one purple team event, then before you know it was back to red vs blue? Or maybe your purple team just never happened? Join Allie as she discusses her experiences with this struggle - where she dealt with only taking red team reports to make the blue team better, to finally getting them to collaborate and improve both teams!

SpeakerBio: Allie

Allie is a Senior Security Analyst with eight years of combined experience across systems administration, networking, and cybersecurity. She has previously presented work about threat hunting nation state actors targeting the open-source software ecosystem. She spends her days hunting threat actors and leading incident response investigations. Outside of work, she enjoys camping, spending time with her dog, and her kids, who rank somewhere between "favorite humans" and "active incident response scenario" depending on the day.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

DEF CON Training - Tuesday - 08:30-17:30 PDT

Title: Deep Dive into the Dark Web

Tags: DEF CON Training (Paid) (2-day) | DEF CON Training

When: Tuesday, Aug 11, 08:30 - 17:30 PDT

Where: LVCCW Level 2 W221 (Training) - [Map](#)

Description:

SpeakerBio: Robert "pwcraack" Weiss

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

DEF CON Training - Monday - 08:30-17:30 PDT

Title: Deep Dive into the Dark Web

Tags: DEF CON Training (Paid) (2-day) | DEF CON Training

When: Monday, Aug 10, 08:30 - 17:30 PDT

Where: LVCCW Level 2 W221 (Training) - [Map](#)

Description:

SpeakerBio: Robert "pwcraack" Weiss

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Payment Village - Friday - 15:00-15:45 PDT

Title: Deepfake Detection Through Adversarial Research

Tags: Payment Village | Creator Talk/Panel

When: Friday, Aug 7, 15:00 - 15:45 PDT

Where: LVCCW Level 2 W204-205 (Payment Village) - [Map](#)

Description:

Deepfake defense is no longer just a matter of classifying media as real or fake. As attackers adopt new generators, optimize them for specific targets, and automate feedback-driven attack loops, the threat is evolving into agentic fraud. This talk presents an adversarial research approach to defending live identity-verification systems: continuously simulating realistic attacks, generating and evaluating domain-specific synthetic media, turning detector failures into new evaluation data, monitoring emerging tools, and rapidly adapting to unseen generators without overfitting to the latest attack. Ultimately, effective defense requires treating deepfake detection not as a static model-building task, but as a continuously evolving adversarial process in which success is measured by resilience against the next attack, not performance on the last one. We'll extend these concepts in the village through a hands-on challenge, inviting participants to evaluate a blind synthetic-data discrimination task, which illustrates the practical challenges of evaluating increasingly capable adversarials.

SpeakerBio: Efim Boieru, Senior Manager of ML Engineering, Incode Technologies

10+ years in applied AI, computer vision and biometric security, focused on face liveness and deepfake detection; previously in ML research/engineering roles at Huawei and Bosch.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Payment Village - Saturday - 14:30-15:15 PDT

Title: Deepfake Detection Through Adversarial Research

Tags: Payment Village | Creator Talk/Panel

When: Saturday, Aug 8, 14:30 - 15:15 PDT

Where: LVCCW Level 2 W204-205 (Payment Village) - [Map](#)

Description:

Deepfake defense is no longer just a matter of classifying media as real or fake. As attackers adopt new generators, optimize them for specific targets, and automate feedback-driven attack loops, the threat is evolving into agentic fraud. This talk presents an adversarial research approach to defending live identity-verification systems: continuously simulating realistic attacks, generating and evaluating domain-specific synthetic media, turning detector failures into new evaluation data, monitoring emerging tools, and rapidly adapting to unseen generators without overfitting to the latest attack. Ultimately, effective defense requires treating deepfake detection not as a static model-building task, but as a continuously evolving adversarial process in which success is measured by resilience against the next attack, not performance on the last one. We'll extend these concepts in the village through a hands-on challenge, inviting participants to evaluate a blind synthetic-data discrimination task, which illustrates the practical challenges of evaluating increasingly capable adversarials.

SpeakerBio: Efim Boieru, Senior Manager of ML Engineering, Incode Technologies

10+ years in applied AI, computer vision and biometric security, focused on face liveness and deepfake detection; previously in ML research/engineering roles at Huawei and Bosch.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

The Diana Initiative - Friday - 12:00-12:10 PDT

Title: DEF CON Academy Tour

Tags: The Diana Initiative | Creator Tour

When: Friday, Aug 7, 12:00 - 12:10 PDT

Where: LVCCW Level 1 South Lobby / Atrium - [Map](#)

Description:

Interested in visiting DEF CON Academy but afraid to go by yourself? The Diana Initiative is hosting tours! Follow a volunteer to DEF CON Academy and be introduced to the community and activities inside!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Social Gatherings/Events - Sunday - 22:30-01:59 PDT

Title: DEF CON After party @ LIV Fontainebleau

Tags: Party

When: Sunday, Aug 9, 22:30 - 01:59 PDT

Where: LIV Nightclub at Fontainebleau

Description:

Close out DEF CON at [LIV Fontainebleau](#). Bring your DEF CON badge for free admission and a free drink.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Contests - Friday - 14:00-14:59 PDT

Title: DEF CON Beard and Mustache Contest

Tags: DEF CON Beard and Mustache Contest | Contest

When: Friday, Aug 7, 14:00 - 14:59 PDT

Where: LVCCW Level 1 Hall 1 100 (Contest Stage) - [Map](#)

Description:

The DC Beard and Mustache Contest has been held every year since DEF CON 19 in 2011 (R.I.P. Riviera), (Except during that COVID thing - but we are not going to talk about that COVID thing), the DEF CON Beard and Mustache Contest highlights the intersection of facial hair and hacker culture.

Participant Prerequisites

For 2025 offering 4 categories for the competition - You may only enter one category.

This is an in-person contest - you must be present to participate.

Full beard: Self-explanatory, for the truly bearded.

Partial Beard: For those sporting Van Dykes, Goatees, Mutton Chops, and other partial beard styles.

Mustache only: Judging on the mustache only, even if bearded. Bring your Handlebars, Fu Manchus, or whatever adorns your upper lip.

Freestyle: Anything goes, including fake and creatively adorned beards. Creative women often do well in the Freestyle category.

Timing

Setup begins 1 hour before the event, on the Contest Stage.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

DEF CON Talks - Sunday - 15:00-17:30 PDT

Title: DEF CON Closing Ceremonies & Awards

Tags: DEF CON Official Talk

When: Sunday, Aug 9, 15:00 - 17:30 PDT

Where: LVCCW Level 1 Hall 3 1006,904 (Main Tracks 1,4) - [Map](#)

Description:

SpeakerBio: Jeff "The Dark Tangent" Moss

Mr. Moss is an internet security expert and is the founder of both the Black Hat Briefings and DEF CON Hacking conferences.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Contests - Friday - 10:00-17:59 PDT

Title: DEF CON CTF: Benevolent Bureau of Birds

Tags: DEF CON CTF: Benevolent Bureau of Birds | Contest

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 2 500 (DEF CON CTF: Benevolent Bureau of Birds) - [Map](#)

Description:

We are the Benevolent Bureau of Birds (BBB), formulated from previous victors of past DEF CON CTF contests. We are dedicated to the ethos at the core of CTF: community, skill-building, and showing off insane new hacking talent.

Participant Prerequisites

Players will have to be qualified by an online qualifer to take place in May. Chosen players are then required to have a laptop to participate in the in-person contest, to interact with the scoreboard and challenges hosted on network.

Pre-Qualification

Yes - online pre-qualifier in May 22-24, 2026.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Contests - Sunday - 10:00-11:59 PDT

Title: DEF CON CTF: Benevolent Bureau of Birds

Tags: DEF CON CTF: Benevolent Bureau of Birds | Contest

When: Sunday, Aug 9, 10:00 - 11:59 PDT

Where: LVCCW Level 1 Hall 2 500 (DEF CON CTF: Benevolent Bureau of Birds) - [Map](#)

Description:

We are the Benevolent Bureau of Birds (BBB), formulated from previous victors of past DEF CON CTF contests. We are dedicated to the ethos at the core of CTF: community, skill-building, and showing off insane new hacking talent.

Participant Prerequisites

Players will have to be qualified by an online qualifer to take place in May. Chosen players are then required to have a laptop to participate in the in-person contest, to interact with the scoreboard and challenges hosted on network.

Pre-Qualification

Yes - online pre-qualifier in May 22-24, 2026.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Contests - Saturday - 10:00-17:59 PDT

Title: DEF CON CTF: Benevolent Bureau of Birds

Tags: DEF CON CTF: Benevolent Bureau of Birds | Contest

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 2 500 (DEF CON CTF: Benevolent Bureau of Birds) - [Map](#)

Description:

We are the Benevolent Bureau of Birds (BBB), formulated from previous victors of past DEF CON CTF contests. We are dedicated to the ethos at the core of CTF: community, skill-building, and showing off insane new hacking talent.

Participant Prerequisites

Players will have to be qualified by an online qualifer to take place in May. Chosen players are then required to have a laptop to participate in the in-person contest, to interact with the scoreboard and challenges hosted on network.

Pre-Qualification

Yes - online pre-qualifier in May 22-24, 2026.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: DEF CON Franklin: What worked, what didn't, and how we are giving agency to water utilities at the top of every bad guy's target list because of data centers

Tags: DEF CON Official Talk

When: Saturday, Aug 8, 17:30 - 20:30 PDT

Where: LVCCW Level 1 Hall 3 904 (Main Track 4) - [Map](#)

Description:

How did DEF CON Franklin's cyber volunteers helped American water systems become more secure as they rise to the top of adversaries' target lists? This talk by Franklin co-founder Jake Braun will outline the program, share success stories from volunteer engagements, and discuss lessons learned from the past year of deployments. The session will also cover Franklin's expansion into new states, highlight findings from the DEF CON Hackers' Almanack, and examine why leading security tools struggle to meet the needs of resource-constrained water systems. Finally, the talk will lay out a path to scaling cybersecurity for water systems nationwide through a centrally managed network of regional MSSPs, and how the DEF CON community can help build it from the ground up.

SpeakerBio: Jake Braun, DEF CON Franklin

Jake Braun is the co-founder of DEF CON Franklin and the Executive Director of the Cyber Policy Initiative at the University of Chicago Harris School of Public Policy. He most recently served in the White House as acting Principal Deputy National Cyber Director. While at the White House, he oversaw the implementation of the National Cybersecurity Strategy, including efforts to secure our water systems, modernize the federal cyber workforce, enhance cyber cooperation with allied nations, and develop AI cybersecurity policy.

In addition to his role at the University of Chicago, Mr. Braun co-founded the DEF CON Voting Machine Hacking Village. In that capacity, he co-authored two award-winning reports on the cyber security of our election infrastructure: the DEF CON 25 and 26 Voting Village Reports. Most recently, he partnered with DEF CON, the world's largest and longest running hacker conference, to launch "DEF CON Franklin," a program to memorialize the most innovative and impactful findings from DEF CON in the annual "Hackers' Almanack." "DEF CON Franklin" also recruits cyber volunteers to support underresourced critical infrastructure.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

The Diana Initiative - Friday - 13:20-13:30 PDT

Title: DEF CON Groups (DCG) Tour

Tags: The Diana Initiative | Creator Tour

When: Friday, Aug 7, 13:20 - 13:30 PDT

Where: LVCCW Level 1 South Lobby / Atrium - [Map](#)

Description:

Interested in visiting DEF CON Groups (DCG) but afraid to go by yourself? The Diana Initiative is hosting tours! Follow a volunteer to DEF CON Groups (DCG) and be introduced to the community and activities inside!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

DEF CON Groups - Sunday - 10:00-13:59 PDT

Title: DEF CON Groups (DCG)

Tags: DEF CON Groups | Creator Event/Activity

When: Sunday, Aug 9, 10:00 - 13:59 PDT

Where: LVCCW Level 2 W238 (DEF CON Groups) - [Map](#)

Description:

DEF CON Groups are the year round, local communities that bring the DEF CON spirit home. Run by volunteers around the world, DCGs create spaces where hackers meet, learn, collaborate, and build community outside of conference season.

The DEF CON Groups community space brings together Points of Contact, members, and prospective members to collaborate, share ideas, and learn from one another. Through informal workshops and hands on interaction, participants exchange practical lessons on building, sustaining, and evolving local hacker communities.

The space also serves as a social anchor. A relaxed place to reconnect with old friends, meet new ones, and participate in light interactive activities that reflect the collaborative nature of hacking culture.

DEF CON has always been the island of misfit toys we all return to once a year. DEF CON Groups are how that ethos survives the other fifty one weeks.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

DEF CON Groups - Saturday - 10:00-17:59 PDT

Title: DEF CON Groups (DCG)

Tags: DEF CON Groups | Creator Event/Activity

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 2 W238 (DEF CON Groups) - [Map](#)

Description:

DEF CON Groups are the year round, local communities that bring the DEF CON spirit home. Run by volunteers around the world, DCGs create spaces where hackers meet, learn, collaborate, and build community outside of conference season.

The DEF CON Groups community space brings together Points of Contact, members, and prospective members to collaborate, share ideas, and learn from one another. Through informal workshops and hands on interaction, participants exchange practical lessons on building, sustaining, and evolving local hacker communities.

The space also serves as a social anchor. A relaxed place to reconnect with old friends, meet new ones, and participate in light interactive activities that reflect the collaborative nature of hacking culture.

DEF CON has always been the island of misfit toys we all return to once a year. DEF CON Groups are how that ethos survives the other fifty one weeks.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

DEF CON Groups - Friday - 10:00-17:59 PDT

Title: DEF CON Groups (DCG)

Tags: DEF CON Groups | Creator Event/Activity

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 2 W238 (DEF CON Groups) - [Map](#)

Description:

DEF CON Groups are the year round, local communities that bring the DEF CON spirit home. Run by volunteers around the world, DCGs create spaces where hackers meet, learn, collaborate, and build community outside of conference season.

The DEF CON Groups community space brings together Points of Contact, members, and prospective members to collaborate, share ideas, and learn from one another. Through informal workshops and hands on interaction, participants exchange practical lessons on building, sustaining, and evolving local hacker communities.

The space also serves as a social anchor. A relaxed place to reconnect with old friends, meet new ones, and participate in light interactive activities that reflect the collaborative nature of hacking culture.

DEF CON has always been the island of misfit toys we all return to once a year. DEF CON Groups are how that ethos survives the other fifty one weeks.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

DEF CON Groups - Thursday - 10:00-17:59 PDT

Title: DEF CON Groups (DCG)

Tags: DEF CON Groups | Creator Event/Activity

When: Thursday, Aug 6, 10:00 - 17:59 PDT

Where: LVCCW Level 2 W238 (DEF CON Groups) - [Map](#)

Description:

DEF CON Groups are the year round, local communities that bring the DEF CON spirit home. Run by volunteers around the world, DCGs create spaces where hackers meet, learn, collaborate, and build community outside of conference season.

The DEF CON Groups community space brings together Points of Contact, members, and prospective members to collaborate, share ideas, and learn from one another. Through informal workshops and hands on interaction, participants exchange practical lessons on building, sustaining, and evolving local hacker communities.

The space also serves as a social anchor. A relaxed place to reconnect with old friends, meet new ones, and participate in light interactive activities that reflect the collaborative nature of hacking culture.

DEF CON has always been the island of misfit toys we all return to once a year. DEF CON Groups are how that ethos survives the other fifty one weeks.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Contests - Saturday - 10:00-17:59 PDT

Title: DEF CON Groups Backdoors & Breaches

Tags: DEF CON Groups | DEF CON Groups Backdoor & Breaches | Contest

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 2 W238 (DEF CON Groups) - [Map](#)

Description:

Tournament-Style Backdoors & Breaches Competitive – Live Incident Response Showdowns The DEF CON Groups Community is bringing live, bracket-style Backdoors & Breaches Competitive Games to DEF CON 34. Backdoors & Breaches is an incident response card game built around realistic breach scenarios. In our tournament format, teams step into the roles of adversaries, where they will take turns attacking or defending against each other. They must analyze scenarios, identify adversarial tactics, make technical and business decisions, and mitigate damage before attackers wipe them out of the game. This isn't passive content. This is live, projected, real-time decision-making. Matches will be bracketed and displayed on screen so attendees can watch strategies unfold, debate choices, and learn from both brilliant plays and catastrophic missteps. Spectators become students of the game — observing how attacks progress, how defenders prioritize, and how communication and leadership shape outcomes. Participants can:

- Join the tournament on the spot — no pre-qualifiers required
- Compete in structured brackets
- Win donated swag
- Learn incident response by doing, not just listening

What will you learn? You'll see how modern attacks move from initial access to impact. You'll experience the tension of limited funding. You'll learn how small decisions compound during an incident. You'll understand how legal, executive, and technical perspectives collide in a breach scenario. Most importantly, you'll build intuition for thinking like both attackers and defenders. This is hacking culture through simulation: adversary thinking, defensive strategy, rapid analysis, and creative problem solving — all wrapped in competition. Located inside the DCG Community space, the tournament creates visible energy and draws attendees into a broader ecosystem of DEF CON Groups, workshops, sticker contests, and community collaboration. If you've ever wanted to see incident response as a spectator sport — or test your instincts under pressure — pull up a chair.

Speakers:Tim Doerges,Seth Benning

SpeakerBio: Tim Doerges, Lead Developer | Backdoors & Breaches at Black Hills Information Security

Tim Doerges is the Lead Developer for Backdoors & Breaches at Black Hills Information Security and will facilitate the live tournament-style matches at DEF CON 34.

SpeakerBio: Seth Benning, Product Developer at Black Hills Information Security

Seth Benning is an Assistant Conference Coordinator and Product Developer with Wild West Hackin' Fest and Black Hills Information Security. He will help facilitate the Backdoors & Breaches tournament at DEF CON 34.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: DEF CON Groups Backdoors & Breaches

Tags: DEF CON Groups | DEF CON Groups Backdoor & Breaches | Contest

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 2 W238 (DEF CON Groups) - [Map](#)

Description:

Tournament-Style Backdoors & Breaches Competitive – Live Incident Response Showdowns The DEF CON Groups Community is bringing live, bracket-style Backdoors & Breaches Competitive Games to DEF CON 34. Backdoors & Breaches is an incident response card game built around realistic breach scenarios. In our tournament format, teams step into the roles of adversaries, where they will take turns attacking or defending against each other. They must analyze scenarios, identify adversarial tactics, make technical and business decisions, and mitigate damage before attackers wipe them out of the game. This isn't passive content. This is live, projected, real-time decision-making. Matches will be bracketed and displayed on screen so attendees can watch strategies unfold, debate choices, and learn from both brilliant plays and catastrophic missteps. Spectators become students of the game — observing how attacks progress, how defenders prioritize, and how communication and leadership shape outcomes. Participants can:

- Join the tournament on the spot — no pre-qualifiers required
- Compete in structured brackets
- Win donated swag
- Learn incident response by doing, not just listening

What will you learn? You'll see how modern attacks move from initial access to impact. You'll experience the tension of limited funding. You'll learn how small decisions compound during an incident. You'll understand how legal, executive, and technical perspectives collide in a breach scenario. Most importantly, you'll build intuition for thinking like both attackers and defenders. This is hacking culture through simulation: adversary thinking, defensive strategy, rapid analysis, and creative problem solving — all wrapped in competition. Located inside the DCG Community space, the tournament creates visible energy and draws attendees into a broader ecosystem of DEF CON Groups, workshops, sticker contests, and community collaboration. If you've ever wanted to see incident response as a spectator sport — or test your instincts under pressure — pull up a chair.

Speakers:Tim Doerges,Seth Benning

SpeakerBio: Tim Doerges, Lead Developer | Backdoors & Breaches at Black Hills Information Security

Tim Doerges is the Lead Developer for Backdoors & Breaches at Black Hills Information Security and will facilitate the live tournament-style matches at DEF CON 34.

SpeakerBio: Seth Benning, Product Developer at Black Hills Information Security

Seth Benning is an Assistant Conference Coordinator and Product Developer with Wild West Hackin' Fest and Black Hills Information Security. He will help facilitate the Backdoors & Breaches tournament at DEF CON 34.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: DEF CON Groups Sticker Contest

Tags: DEF CON Groups | DEF CON Groups Sticker Contest | Contest

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 2 W238 (DEF CON Groups) - [Map](#)

Description:

The DCG Sticker Contest is a sticker design contest with winner by popular vote and voting happening during DEF CON 34.

Anyone can submit original, human-created sticker designs prior to DEF CON 34. During DC34 attendees view all entries on site, and vote in person for their favorites. Designs will be displayed in the DEF CON Groups Community space throughout the conference, with voting open on Thursday to Saturday and the winning design announced on Sunday.

Stickers are hacker currency. This contest is about celebrating that culture through creativity, participation, and community choice. The top designs go through to the voting round. What wins is what the DEF CON community votes for.

Whether you want to support fellow hackers, or help decide the winning design, this is your chance to participate directly.

Participant Prerequisites

For designers / contributors: - Original sticker artwork created by a human (no AI-generated art) - You may design it yourself or work with a human graphic designer - Ability to submit artwork digitally prior to DEF CON - No specialized technical knowledge required

For voters: - Attendance at DEF CON - Ability to view entries in person and cast a vote - Voting is honor-based: one human, one vote - Participants may vote

No special hardware, software, or prior experience is required to participate or vote.

Pre-Qualification

A call for sticker designs will open prior to DEF CON with the contest and voting happening on-site.

Activity schedule: Thursday setup and preview; Friday and Saturday active voting; contest winner announced Sunday on the Contest Stage. See the Hacker Tracker Contest Stage entry for announcement details.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Contests - Saturday - 10:00-17:59 PDT

Title: DEF CON Groups Sticker Contest

Tags: DEF CON Groups | DEF CON Groups Sticker Contest | Contest

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 2 W238 (DEF CON Groups) - [Map](#)

Description:

The DCG Sticker Contest is a sticker design contest with winner by popular vote and voting happening during DEF CON 34.

Anyone can submit original, human-created sticker designs prior to DEF CON 34. During DC34 attendees view all entries on site, and vote in person for their favorites. Designs will be displayed in the DEF CON Groups Community space throughout the conference, with voting open on Thursday to Saturday and the winning design announced on Sunday.

Stickers are hacker currency. This contest is about celebrating that culture through creativity, participation, and community choice. The top designs go through to the voting round. What wins is what the DEF CON community votes for.

Whether you want to support fellow hackers, or help decide the winning design, this is your chance to participate directly.

Participant Prerequisites

For designers / contributors: - Original sticker artwork created by a human (no AI-generated art) - You may design it yourself or work with a human graphic designer - Ability to submit artwork digitally prior to DEF CON - No specialized technical knowledge required

For voters: - Attendance at DEF CON - Ability to view entries in person and cast a vote - Voting is honor-based: one human, one vote - Participants may vote

No special hardware, software, or prior experience is required to participate or vote.

Pre-Qualification

A call for sticker designs will open prior to DEF CON with the contest and voting happening on-site.

Activity schedule: Thursday setup and preview; Friday and Saturday active voting; contest winner announced Sunday on the Contest Stage. See the Hacker Tracker Contest Stage entry for announcement details.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Contests - Sunday - 10:00-11:59 PDT

Title: DEF CON Scavenger Hunt

Tags: DEF CON Scavenger Hunt | Contest

When: Sunday, Aug 9, 10:00 - 11:59 PDT

Where: LVCCW Level 1 Hall 1 104 (DEF CON Scavenger Hunt) - [Map](#)

Description:

Whether you're a seasoned DEF CON veteran or a curious newcomer, the DEF CON Scavenger Hunt promises to challenge your skills, tickle your wits, and ignite your hacker spirit. Our list is a portal to mystery, mischief, and mayhem. Assemble your team of up to 5 members, interpret the items, and submit your efforts at the booth to our esteemed judges. Go beyond the basics for bonus points. Legends are born here.

The DEF CON Scavenger Hunt is open to everyone, regardless of skill level or experience, no pre-qualifying necessary. We strive to maintain the balance of a low barrier to entry while providing a challenge that many are eager to take on. Casual players should not be overwhelmed by the list, find a handful of items and have fun. If you are looking to win however, you will need to fully immerse yourself in the DEF CON Scavenger Hunt. Let's make some memories together.

Remember that it's not just about fame, glory, or boxes of swag; the true allure is the camaraderie of fellow hackers, the knowledge that you've etched your mark on DEF CON history, and the ultimate badge of honor: bragging rights. Nothing says "I'm a hacker" quite like being triumphant at the DEF CON Scavenger Hunt.

Participant Prerequisites

No, we work very hard to maintain a very low barrier to entry. If anything is required for an item, they should be able to find a fellow hacker with it that would be willing to assist them with their item.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Contests - Saturday - 10:00-17:59 PDT

Title: DEF CON Scavenger Hunt

Tags: DEF CON Scavenger Hunt | Contest

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 104 (DEF CON Scavenger Hunt) - [Map](#)

Description:

Whether you're a seasoned DEF CON veteran or a curious newcomer, the DEF CON Scavenger Hunt promises to challenge your skills, tickle your wits, and ignite your hacker spirit. Our list is a portal to mystery, mischief, and mayhem. Assemble your team of up to 5 members, interpret the items, and submit your efforts at the booth to our esteemed judges. Go beyond the basics for bonus points. Legends are born here.

The DEF CON Scavenger Hunt is open to everyone, regardless of skill level or experience, no pre-qualifying necessary. We strive to maintain the balance of a low barrier to entry while providing a challenge that many are eager to take on. Casual players should not be overwhelmed by the list, find a handful of items and have fun. If you are looking to win however, you will need to fully immerse yourself in the DEF CON Scavenger Hunt. Let's make some memories together.

Remember that it's not just about fame, glory, or boxes of swag; the true allure is the camaraderie of fellow hackers, the knowledge that you've etched your mark on DEF CON history, and the ultimate badge of honor: bragging rights. Nothing says "I'm a hacker" quite like being triumphant at the DEF CON Scavenger Hunt.

Participant Prerequisites

No, we work very hard to maintain a very low barrier to entry. If anything is required for an item, they should be able to find a fellow hacker with it that would be willing to assist them with their item.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: DEF CON Scavenger Hunt

Tags: DEF CON Scavenger Hunt | Contest

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 104 (DEF CON Scavenger Hunt) - [Map](#)

Description:

Whether you're a seasoned DEF CON veteran or a curious newcomer, the DEF CON Scavenger Hunt promises to challenge your skills, tickle your wits, and ignite your hacker spirit. Our list is a portal to mystery, mischief, and mayhem. Assemble your team of up to 5 members, interpret the items, and submit your efforts at the booth to our esteemed judges. Go beyond the basics for bonus points. Legends are born here.

The DEF CON Scavenger Hunt is open to everyone, regardless of skill level or experience, no pre-qualifying necessary. We strive to maintain the balance of a low barrier to entry while providing a challenge that many are eager to take on. Casual players should not be overwhelmed by the list, find a handful of items and have fun. If you are looking to win however, you will need to fully immerse yourself in the DEF CON Scavenger Hunt. Let's make some memories together.

Remember that it's not just about fame, glory, or boxes of swag; the true allure is the camaraderie of fellow hackers, the knowledge that you've etched your mark on DEF CON history, and the ultimate badge of honor: bragging rights. Nothing says "I'm a hacker" quite like being triumphant at the DEF CON Scavenger Hunt.

Participant Prerequisites

No, we work very hard to maintain a very low barrier to entry. If anything is required for an item, they should be able to find a fellow hacker with it that would be willing to assist them with their item.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Social Gatherings/Events - Thursday - 06:00-07:59 PDT

Title: Defcon.run

Tags: Event

When: Thursday, Aug 6, 06:00 - 07:59 PDT

Where: LVCCW Level 1 North Entrance - [Map](#)

Description:

Defcon.run, formerly the DEF CON 4x5K, is a community-driven tradition where hackers gather for morning runs and rucks across Las Vegas. Participants can choose from various routes, from 5Ks to longer distances.

For DEF CON 34, meet at "The Spot" near the North Entrance of the Las Vegas Convention Center West Hall. Activities start at 06:00, Thursday through Sunday; arrive early for safety briefings and community hype.

Whether you are an experienced runner or a newcomer, visit [defcon.run](#) to sign up and connect with the community.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Social Gatherings/Events - Saturday - 06:00-07:59 PDT

Title: Defcon.run

Tags: Event

When: Saturday, Aug 8, 06:00 - 07:59 PDT

Where: LVCCW Level 1 North Entrance - [Map](#)

Description:

Defcon.run, formerly the DEF CON 4x5K, is a community-driven tradition where hackers gather for morning runs and rucks across Las Vegas. Participants can choose from various routes, from 5Ks to longer distances.

For DEF CON 34, meet at "The Spot" near the North Entrance of the Las Vegas Convention Center West Hall. Activities start at 06:00, Thursday through Sunday; arrive early for safety briefings and community hype.

Whether you are an experienced runner or a newcomer, visit [defcon.run](#) to sign up and connect with the community.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Social Gatherings/Events - Sunday - 06:00-07:59 PDT

Title: Defcon.run

Tags: Event

When: Sunday, Aug 9, 06:00 - 07:59 PDT

Where: LVCCW Level 1 North Entrance - [Map](#)

Description:

Defcon.run, formerly the DEF CON 4x5K, is a community-driven tradition where hackers gather for morning runs and rucks across Las Vegas. Participants can choose from various routes, from 5Ks to longer distances.

For DEF CON 34, meet at "The Spot" near the North Entrance of the Las Vegas Convention Center West Hall. Activities start at 06:00, Thursday through Sunday; arrive early for safety briefings and community hype.

Whether you are an experienced runner or a newcomer, visit [defcon.run](#) to sign up and connect with the community.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Social Gatherings/Events - Friday - 06:00-07:59 PDT

Title: Defcon.run

Tags: Event

When: Friday, Aug 7, 06:00 - 07:59 PDT

Where: LVCCW Level 1 North Entrance - [Map](#)

Description:

Defcon.run, formerly the DEF CON 4x5K, is a community-driven tradition where hackers gather for morning runs and rucks across Las Vegas. Participants can choose from various routes, from 5Ks to longer distances.

For DEF CON 34, meet at "The Spot" near the North Entrance of the Las Vegas Convention Center West Hall. Activities start at 06:00, Thursday through Sunday; arrive early for safety briefings and community hype.

Whether you are an experienced runner or a newcomer, visit [defcon.run](#) to sign up and connect with the community.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Defend zee clankers: OWASP AI Security Verification Standard (AISVS)

Tags: OWASP Foundation | Creator Talk/Panel

When: Friday, Aug 7, 14:30 - 15:15 PDT

Where: LVCCW Level 1 Hall 3 1100 (Creator Stage 7) - [Map](#)

Description:

AI systems face threats that traditional application security standards weren't built to address. This includes prompt injection, training data poisoning, model extraction, agentic autonomy risks, and more. The OWASP AI Security Verification Standard (AISVS) provides 400+ testable requirements across 14 chapters, covering everything from input validation and model lifecycle management to MCP protocol security and autonomous agent controls. This lightning talk introduces the standard's structure, its three verification levels, and how security teams can use it today to assess and harden AI-powered applications. We'll show where AISVS fits alongside existing frameworks like ASVS, NIST AI RMF, and ISO 42001 and where it deliberately doesn't overlap.

SpeakerBio: Jim Manico, Founder at Manicode Security

Jim Manico is the founder of Manicode Security, where he specializes in training software developers on secure coding and security engineering. He is actively involved in multiple ventures, serving as an investor/advisor for companies like 10Security, MergeBase, Nucleus Security, KSOC, and Inspectiv, among others. Jim is a recognized speaker, focusing on secure software practices, and holds a distinguished position as a member of the Java Champion community. He is also the esteemed author of "Iron-Clad Java: Building Secure Web Applications" published by Oracle Press.

Additionally, Jim generously volunteers for the OWASP foundation, co-leading key projects such as the OWASP Application Security Verification Standard and the OWASP Cheatsheet Series.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Defense in Depth for AI: Launching the AISECA Framework

Tags: Middle Easterns & Africans in Cyber Security (MEACS) | Creator Talk/Panel

When: Friday, Aug 7, 16:00 - 16:59 PDT

Where: LVCCW Level 1 Hall 4 1306 (Middle Easterns & Africans in Cyber Security (MEACS) Community) - [Map](#)

Description:

Every week brings a new agentic AI attack and a new point solution that claims to stop it. None of them stop all of it, because agents do not have one attack surface, they have many, spread across the skills they load, the tools they call, the data they touch, and the humans who approve them. This talk introduces the AISECA Tiered Control Framework, an open, community-built model for defending agentic workflows the way we defend everything else that matters: in depth, in layers, with no single control carrying the whole load. We walk the framework end to end, then go deep on one control to show how it works in practice, what it catches, what it misses, and how it composes with the controls around it. You will leave with a shared vocabulary for agentic risk and a practical way to find the gaps in your own stack. Built in the open by practitioners, free to adopt, and yours to extend.

Speakers: Amber Bennoui, Karol Piekarski

SpeakerBio: Amber Bennoui

No BIO available

SpeakerBio: Karol Piekarski, DevOps Engineer

Karol Piekarski is a Lead DevOps Engineer working across cloud infrastructure, zero-trust architecture, and AI and agentic security for systems that serve hundreds of millions of consumers. His research focuses on the security of large language models and autonomous agents, with an emphasis on practical red-teaming and defensive tooling that teams can actually operationalize rather than shelve.

His empirical work on ablation and agentic framing reframes where alignment actually breaks down in agent pipelines: agentic framing alone can collapse a model's baseline safety, while ablation matters mostly for the hardest content and is highly architecture-dependent. In 2026 he co-presented "Move Fast, Stay Secure: Enterprise AI Agent Security in Practice" at the Databricks Data + AI Summit, and spoke at SCALE 23x on open source red-teaming for LLMs. He was one of only two external contributors to the Databricks Agentic AI Security Framework (DASF v3.0).

Karol is the creator of Sundew.sh, an open source, MCP-native AI agent honeypot platform that uses behavioral fingerprinting and a persona engine for anti-fingerprinting, now adopted by external research teams studying agent behavior in the wild. He was selected as a Wiz MVP last year and this year received Wiz's Thought Leader award, and he is active in the AISECA Working Group, where he co-owns agentic security risk definitions.

He holds the CCSP, CKA, four AWS specialty certifications along with DataDog and Tines, and he regularly judges and mentors at hackathons across Southern California.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Demodus Operandi (Cómo tres rf-hacks en tres bandas terminaron siendo una metodología)

Tags: La Villa Community | Creator Talk/Panel

When: Friday, Aug 7, 11:30 - 12:30 PDT

Where: LVCCW Level 1 Hall 4 1416 (La Villa Community) Main Stage - [Map](#)

Description:

Hay muchas herramientas para hackear RF y mucho conocimiento regado en talks, repos y la cabeza de la gente. Lo que no hay es un mapa. Cuando te paras frente a un dispositivo o señal, ¿por dónde empiezas? ¿y cómo sabes qué se te escapó?

Esta charla cubre tres investigaciones reales, cada una en una tecnología distinta.

Primero BLE, sniffendo advertising packets terminé auditando una sala y encontré 6 de 85 dispositivos completamente controlables, incluso con LE Secure Connections habilitado.

Después LoRaWAN, capturé 51,304 frames en US915. El 89.3% eran JoinRequests: una red entera fallando en unirse, visible sin transmitir un solo paquete, red que no podía encontrar con un SDR.

Y al final LTE — encontrar la celda correcta en México, entender el OFDM, y extraer metadatos en pasivo.

Tres casos, tres analisis distintos. Pero siempre sobre las mismas capas: espectro señal enlace cripto ataque.

Ya seguía una metodología, solo no la había nombrado.

Así nació RFSAM (Radio Frequency Security Assessment Methodology): una referencia abierta, estructurada, que organiza lo que OSSTMM, BSAM y la comunidad SDR ya construyeron, en algo que puedes navegar. No pretende inventar nada, pretende ser un mapa.

<https://electroniccats.github.io/RFSAM/>

SpeakerBio: Eduardo Contreras, CTO

Electronics Engineer, passionate about technological development

and science, co-founder and CTO of the Electronic Cats company which has developed different embedded systems already in production, focused from education to security related devices, embedded programmer, has developed open source libraries for communities as well as open hardware, with the goal to design and implement global impact electronics.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Demystifying the Playboy RaaS

Tags: Malware Village | Creator Talk/Panel

When: Saturday, Aug 8, 10:45 - 11:25 PDT

Where: LVCCW Level 1 Hall 2 600 (Malware Village) Talks - [Map](#)

Description:

In recent years, ransomware has become one of the most prolific forms of cybercrime with financial gain as primary motive. The problem keeps getting bigger, with a new operation seeing the light almost every month. The Dutch National Police is often a key player in large-scale ransomware investigations. Operation Cronos is a prime example, where law enforcement took down infrastructure of the infamous LockBit group in 2024.

Today, many ransomware groups operate RaaS (ransomware-as-a-service) models. They provide the ransomware and a platform to extort victims as a service, and affiliated hacker groups carry out the actual attacks. The platform is often run from a VPS (virtual private server), and sometimes, this server is in the Netherlands. Dutch law enforcement seizes those servers and extracts their content for investigation. This happened to the Playboy ransomware in late 2024.

A chain of various tools is used to provide a ready-to-use ransomware package to affiliates of a RaaS program. Several modern ransomware operations even support CPU architectures and operating systems other than x86-64 and Windows. New cryptographic keys are generated for every victim, ransomware parameters are configured, and a builder creates the final package to be used by the affiliate. In this talk, we will reveal how we seized the Playboy ransomware servers, dive into its toolchain, and look at how executables were prepared to breach victims.

SpeakerBio: Gijs Rijnders, Malware & CTI Specialist

Gijs is a cyber threat intelligence analyst and malware reverse engineer at the Dutch National Police where he defends the Police organization from cyber attacks. He previously worked at the CERT of Tesorion, a Dutch cybersecurity company, where he reverse engineered various ransomware families and published decryption tools to the NoMoreRansom initiative to help victims recover from attacks.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Blacks In Cyber Village - Sunday - 13:00-13:59 PDT

Title: DeNISTifying Technology: Paradigm Shifting To Quantum Encryption, Post Cryptography, and Digital Forensics

Tags: Blacks In Cyber Village | Creator Talk/Panel

When: Sunday, Aug 9, 13:00 - 13:59 PDT

Where: LVCCW Level 3 W322-W324 (BIC Village) - [Map](#)

Description:

Dive into the future of cybersecurity with a session that challenges conventional thinking. This talk explores the concept of 'DeNISTifying Technology,' guiding attendees through paradigm shifts towards quantum encryption, advanced post-cryptography methods, and the evolving landscape of digital forensics. Discover innovative approaches and critical insights into securing our digital world beyond current standards. All experience levels are welcome to explore these cutting-edge topics.

SpeakerBio: Aisha Berry, University of Maryland Global Campus

Aisha Berry is a cybersecurity professional, PhD candidate, and experienced nurse with over 15 years in healthcare. They hold a Bachelor's in Cybersecurity and Computer Networking with a focus on digital forensics, and a Master's of Science in Digital Forensics and Cyber Investigations. Currently pursuing a doctoral program with a focus on healthcare, Aisha delves into the psychological component of technology, emphasizing the mindset of attackers in cybersecurity strategy.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Descubrimiento Industrializado de CVEs con Agentes de IA

Tags: La Villa Community | Creator Talk/Panel

When: Saturday, Aug 8, 12:30 - 13:30 PDT

Where: LVCCW Level 1 Hall 4 1416 (La Villa Community) Main Stage - [Map](#)

Description:

¿De verdad puede la IA encontrar vulnerabilidades reales y nuevas a gran escala? La seguridad de aplicaciones es nuestra disciplina, y somos una CNA de tipo investigador, entre las primeras del CNA Scorecard. Montamos una cadena de producción y la soltamos sobre 36 proyectos de código abierto. Hasta ahora, y contando: 539 hallazgos revisados, depurados hasta 8 CVEs públicos y 30 candidatos a CVE.

La charla recorre la cadena completa: cómo entrenamos agentes que recorren el código, cómo un modelo de machine learning detecta los fragmentos sospechosos, cómo los hackers y researchers validan cada candidato y qué números deja cada etapa del filtrado.

Nuestra meta: acortar el tiempo de detección a escala sin sacrificar exactitud, para que la ventana de exposición (detección + remediación) sea menor que el tiempo de explotación. Te llevas un método replicable para convertir LLMs impredecibles en una fábrica seria de CVEs, con las métricas de precisión que la sostienen.

Speakers: Simon Correa, Michael Rivera

SpeakerBio: Simon Correa, Fluid Attacks, Head of Research

Simón Correa, Head of Research en Fluid Attacks, es responsable de coordinar el CNA de la compañía, realizar investigaciones técnicas de ciberseguridad y liderar la detección de vulnerabilidades en software open source de terceros, gestionando todo el ciclo de vida de los CVEs desde su descubrimiento hasta su publicación. Además, coordina y participa en el equipo interno de CTFs, analizando el rendimiento y diseñando estrategias de mejora para futuras competencias. En su rol, mantiene la interlocución con MITRE y NIST, prepara publicaciones académicas y ponencias para conferencias especializadas, y organiza meetups técnicos que fortalecen el posicionamiento de Fluid Attacks en la comunidad de seguridad.

SpeakerBio: Michael Rivera, Chief Data & AI Officer | M.Sc. in Analytics

Michael Rivera is the Chief Data & AI Officer at Fluid Attacks, where he leads initiatives that combine advanced data analytics and artificial intelligence to strengthen software quality and security. His work in recent years has focused on developing methods that reduce the time required to detect vulnerabilities and on ensuring that AI-driven systems are built under the security-by-design approach.

Michael combines an academic background in economics with his Master of Science in Analytics at the Georgia Institute of Technology, enabling him to bring an uncommon interdisciplinary perspective to the field of cybersecurity. With years of experience bridging data science and AppSec practice, he offers both technical depth and strategic insight, making him uniquely positioned to help organizations adopt rigorous frameworks for evaluating security solutions.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: DFMI: Weaponizing MSI Installers for Fileless Code Execution

Tags: Red Team Village | Misc

When: Sunday, Aug 9, 14:00 - 14:59 PDT

Where: LVCCW Level 1 Hall 1 309 (Red Team Village) Workshop Stage 1 - [Map](#)

Description:

DFMI is a cross-platform, open-source offensive toolkit that hijacks & abuses the Windows Installer's own execution engine to detonate arbitrary payloads during software installation, with zero files written to disk and zero evidence left behind. And this can be achieved without even corrupting the Authenticode of the binary.

The attack surface is the CustomAction table embedded in every MSI database — a small structure that Windows Installer processes unconditionally at install time. DFMI injects a deferred CustomAction (property-based EXE invocation) — firing right before the modification in system files; the payload executes before a single legitimate byte touches the filesystem.

Right now, DFMI provides 3 different methods for abusing MSI files: - Inject: Simply injects a CustomAction (CA) into an existing MSI package. - Rogue MST: Generates an MSI Transform File (.mst) and injects into legitimate ".msi" file without corrupting its Authenticode. - Stub: Creates a malicious MSI file from scratch.

What makes DFMI particularly difficult to eradicate is that it exploits no vulnerability; it's a feature. The CustomAction mechanism is a 25-year-old Windows feature, documented by Microsoft, used by virtually every enterprise software package and trusted implicitly by the OS.

DFMI simply turns that trust sideways — using the Installer engine as its own payload executor.

<https://github.com/ccelikanil/DFMI>

SpeakerBio: Anıl Çelik

Computer Engineer & been working as a Red Teamer for the past ~7 years. Previously did presentations at DEFCON 33 Demo Labs, DEFCON 33 Red Team Village & Black Hat USA Arsenal 2025. Currently holding 6 CVEs, OSCP & OSWP. Interests: Windows Internals & AD Security

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: DFMI: Weaponizing MSI Installers for Fileless Code Execution

Tags: DEF CON Demo Labs | Intermediate | Defense/Blue Team | Malware | Offense/Red Team | Purple Team | Threat Intel/Hunting | DEF CON Demo Labs

When: Saturday, Aug 8, 10:00 - 10:45 PDT

Where: LVCCW Level 1 Hall 3 900 (Demo Labs Track 4) - [Map](#)

Description:

DFMI is a cross-platform, open-source offensive toolkit that hijacks & abuses the Windows Installer's own execution engine to detonate arbitrary payloads during software installation, with zero files written to disk and zero evidence left behind. And this can be achieved without corrupting the Authenticode of the binary. --Which means, ANY signed legitimate installer file can leveraged as an attack vector.

Right now, DFMI provides 3 different methods for abusing MSI files:

- Inject: Simply injects a CustomAction (CA) into an existing MSI package.
- Rogue MST: Generates an MSI Transform File (.mst) and injects into legitimate ".msi" file without corrupting it's Authenticode. The original MSI file is never modified — its Authenticode signature remains fully intact and valid. This means a signed, trusted MSI can be weaponized without leaving any forensic trace on the file itself; the transform rides alongside it at deployment time.
- Stub: Creates a malicious MSI file from scratch.

GitHub: <https://github.com/ccelikanil/DFMI>

SpeakerBio: Anil Celik

Computer Engineer & been working as a Red Teamer for the past ~7 years. Previously did presentations at DEFCON 33 Demo Labs, DEFCON 33 Red Team Village & Black Hat USA Arsenal 2025. Currently holding 6 CVEs, OSCP & OSWP.

Interests: Windows Internals & AD Security

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: DFMI: Weaponizing MSI Installers for Fileless Code Execution

Tags: DEF CON Demo Labs | Intermediate | Defense/Blue Team | Malware | Offense/Red Team | Purple Team | Threat Intel/Hunting | DEF CON Demo Labs

When: Friday, Aug 7, 16:00 - 16:45 PDT

Where: LVCCW Level 1 Hall 3 900 (Demo Labs Track 4) - [Map](#)

Description:

DFMI is a cross-platform, open-source offensive toolkit that hijacks & abuses the Windows Installer's own execution engine to detonate arbitrary payloads during software installation, with zero files written to disk and zero evidence left behind. And this can be achieved without corrupting the Authenticode of the binary. --Which means, ANY signed legitimate installer file can leveraged as an attack vector.

Right now, DFMI provides 3 different methods for abusing MSI files:

- Inject: Simply injects a CustomAction (CA) into an existing MSI package.
- Rogue MST: Generates an MSI Transform File (.mst) and injects into legitimate ".msi" file without corrupting it's Authenticode. The original MSI file is never modified — its Authenticode signature remains fully intact and valid. This means a signed, trusted MSI can be weaponized without leaving any forensic trace on the file itself; the transform rides alongside it at deployment time.
- Stub: Creates a malicious MSI file from scratch.

GitHub: <https://github.com/ccelikanil/DFMI>

SpeakerBio: Anil Celik

Computer Engineer & been working as a Red Teamer for the past ~7 years. Previously did presentations at DEFCON 33 Demo Labs, DEFCON 33 Red Team Village & Black Hat USA Arsenal 2025. Currently holding 6 CVEs, OSCP & OSWP.

Interests: Windows Internals & AD Security

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Blue Team Village - Friday - 12:00-12:59 PDT

Title: Digital Forensics 101

Tags: Blue Team Village | Creator Talk/Panel

When: Friday, Aug 7, 12:00 - 12:59 PDT

Where: LVCCW Level 2 W217 (Blue Team Village) Main Stage - [Map](#)

Description:

Forensics 101 is a fast-paced, story-driven primer on digital investigations—perfect for incident-response newcomers and seasoned blue-teamers alike. In under 45 minutes we trace the full evidence lifecycle: imaging disks and cloud buckets, teasing meaning from volatile memory, and translating binary breadcrumbs into courtroom-ready narratives. First, we demystify the tools and techniques behind solid acquisition and analysis; next, we zoom out to the real-world team dynamics, reporting pitfalls, and career launchpads that turn analysts into trusted advisors. Expect war stories, practical tips you can use on Monday, and zero certification flexing—just the art, science, and occasional 2 a.m. data-center comedy of modern digital forensics.

SpeakerBio: Sarthak Taneja

Started from Offensive Security and ended up in Defense. Wearing Purple hat most of the days.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Digital Modes 101: The Weird, Wonderful World of Computer Radio

Tags: Ham Radio Village | Creator Talk/Panel

When: Saturday, Aug 8, 11:00 - 11:30 PDT

Where: LVCCW Level 3 W315 (Ham Radio Village) - [Map](#)

Description:

Digital communication has become one of the fastest-growing areas of amateur radio. By combining traditional radio equipment with computers and software, operators can send text messages, telemetry, position data, and even digitally encoded voice across the airwaves.

This presentation introduces the fundamentals of amateur radio digital modes and how they work. We'll begin by explaining the difference between analog and digital signals and how computers convert data into audio that radios can transmit.

The talk then explores several widely used digital modes, including FT8 and WSPR for weak-signal communication, JS8Call for keyboard-to-keyboard messaging, and APRS for real-time position tracking and messaging. We'll also look at newer developments such as LoRa-based APRS experimentation and open-source digital voice technologies like FreeDV and M17.

Finally, we'll discuss practical ways to get started with digital radio using affordable hardware, including simple USB radio interfaces, beginner-friendly radios, and lightweight portable setups.

Attendees will leave with a clear understanding of how digital radio works and several easy paths to begin experimenting with digital modes themselves.

Modern amateur radio is no longer just voice communication. Today, radios routinely exchange digital data, text messages, telemetry, and even machine-learning encoded voice signals.

This talk introduces the world of amateur radio digital modes and explains how computers and radios work together to communicate using sound. We'll explore some of the most popular digital modes used by operators today, including FT8, JS8Call, WSPR, APRS, and several emerging digital voice technologies.

Attendees will learn what digital modes are, how they differ from traditional analog radio, and why they have become so popular. The session will also highlight new developments in the digital radio ecosystem, including open-source digital voice systems and long-range LoRa APRS experimentation.

If you've ever wondered what those strange buzzing sounds coming from a radio actually mean—or how to start experimenting with digital radio yourself—this talk will show you how to get started.

SpeakerBio: Jon Marler (K4CHN)

Jon Marler is a cybersecurity product director, hacker, and RF experimenter who enjoys building strange things that connect computers, radios, and networks together. By day he leads security products at VikingCloud focused on protecting global payment infrastructure. By night he experiments with mesh radio networks, hardware hacking, and unconventional communication systems. Jon is particularly interested in how radio and decentralized networks can complement modern security and resilience strategies.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

DEF CON Training - Friday - 08:30-17:30 PDT

Title: Digital Supply Chain Security: Software, Cryptography, AI, and Vendor Risk

Tags: DEF CON Training (Paid) (1-day) | DEF CON Training

When: Friday, Aug 7, 08:30 - 17:30 PDT

Where: LVCCW Level 2 W224 (Training) - [Map](#)

Description:

Speakers: Anant Shrivastava, Sunil Yadav

SpeakerBio: Anant Shrivastava

Anant Shrivastava is the founder of Cyfinoid Research and a long time offensive security practitioner with a focus on application, cloud, and supply chain security. He has delivered trainings and talks at Black Hat (USA, Europe, Asia), Nullcon, c0c0n, BSides, Rootconf and multiple other events, and runs projects such as Hacking Archives of India to highlight real work from the security community. His courses are built from real consulting and red team experience, with an emphasis on attack chains that actually show up in the field and defenses that teams can implement the next day.

SpeakerBio: Sunil Yadav

No BIO available

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Red Team Village - Sunday - 10:00-10:59 PDT

Title: Direct Network Access for Command and Control

Tags: Red Team Village | Misc

When: Sunday, Aug 9, 10:00 - 10:59 PDT

Where: LVCCW Level 1 Hall 1 309 (Red Team Village) Workshop Tactic Table 6 - [Map](#)

Description:

Command and control beacons currently reach out to the operating system to request socket resources, triggering auditing and being restricted by local firewall rules. However, it is possible to develop malware that can evade the standard process. Sparse is a tool that weaponizes this concept to evade such auditing and defensive configurations.

SpeakerBio: Andrew Rioux

I started learning to program in middle school and found a software engineering project to work on throughout highschool. I attended Liberty University to study Software Engineering and Cybersecurity at the undergraduate level, learning to develop software that works in adversarial contexts. I have recently finished my master's degree in Cybersecurity, where I was able to further practice developing software in adversarial contexts and develop version 2 of Sparse



[Return to Index](#) - Add to Google - ics [Calendar](#) file

OSINT For Good Community - Sunday - 11:30-12:45 PDT

Title: Disaster Intelligence - The past, present, and future of situational awareness during a crisis

Tags: OSINT For Good Community | Creator Talk/Panel

When: Sunday, Aug 9, 11:30 - 12:45 PDT

Where: LVCCW Level 1 Hall 4 1307 (OSINT4Good Community) Stage - [Map](#)

Description:

OSINT, social media, drones, AI, and more... in this session, we'll learn how these innovations are applied to make life-saving decisions before, during, and after a disaster

SpeakerBio: Matt Green, Green Emergency Management Services

Matt Green is your friendly neighborhood emergency manager, professor, and host of the state of disaster podcast. His passion is ensuring equitable, high-quality, whole community emergency management across sectors and borders.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

OSINT For Good Community - Sunday - 11:30-11:59 PDT

Title: Disaster Intelligence - The past, present, and future of situational awareness during a crisis

Tags: OSINT For Good Community | Creator Talk/Panel

When: Sunday, Aug 9, 11:30 - 11:59 PDT

Where: LVCCW Level 1 Hall 4 1307 (OSINT4Good Community) Stage - [Map](#)

Description:

OSINT, social media, drones, AI, and more... in this session, we'll learn how these innovations are applied to make life-saving decisions before, during, and after a disaster

SpeakerBio: Matt Green, Green Emergency Management Services

Matt Green is your friendly neighborhood emergency manager, professor, and host of the state of disaster podcast. His passion is ensuring equitable, high-quality, whole community emergency management across sectors and borders.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

IoT Village - Friday - 10:00-17:59 PDT

Title: Discover GE Appliances!

Tags: IoT Village | Creator Event/Activity

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 215 (IoT Village) - [Map](#)

Description:

Join us for a self-guided interactive look at GE Appliances and get hands on with some of our most popular home appliances!



[Return to Index](#) - Add to Google

- ics [Calendar](#) file

IoT Village - Sunday - 10:00-13:59 PDT

Title: Discover GE Appliances!

Tags: IoT Village | Creator Event/Activity

When: Sunday, Aug 9, 10:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 1 215 (IoT Village) - [Map](#)

Description:

Join us for a self-guided interactive look at GE Appliances and get hands on with some of our most popular home appliances!

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

IoT Village - Saturday - 10:00-17:59 PDT

Title: Discover GE Appliances!

Tags: IoT Village | Creator Event/Activity

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 215 (IoT Village) - [Map](#)

Description:

Join us for a self-guided interactive look at GE Appliances and get hands on with some of our most popular home appliances!

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Dissecting the ICX Frog

Tags: Voting Village | Creator Talk/Panel

When: Saturday, Aug 8, 14:30 - 14:59 PDT

Where: LVCCW Level 2 W220 (Voting Village) (Voting Village Talks) - [Map](#)

Description:

In 2022, a Dominion Voting Systems ImageCast X ballot marking device (ICX BMD) appeared for sale on eBay and was purchased by security researcher Harri Hursti. Originating in Colfax Township, MI and after being "donated by accident" to Goodwill, it debuted at Voting Village 2023 and has since been the subject of great interest and used for proof-of-concept demonstrations (PoCs) within the village. As the only known instance of a legally-obtained ICX being available for study without burdensome secrecy/pre-publication review agreements, it represents a unique opportunity for improving and updating our understanding of certified, adopted, and deployed voting systems from an engineering and security perspective (among others).

In this talk, we will discuss the hardware, software, architecture, and capabilities of the ICX BMD from a technical perspective. Significant reverse-engineering of its Democracy Suite 5.5 software has revealed much regarding its design, construction, and internal operation along with a few surprises along the way. While one part of one version of one system from one vendor is far from sufficient to draw conclusions about currently-used voting systems in-general, this talk hopes to shed light on what a currently EAC-approved voting system could be.

SpeakerBio: Drew Springall

Drew Springall is a hacker, security researcher, and frequent Voting Village contributor with a specific interest in the technical/concrete aspects of voting system security. Since 2013, Drew has worked to understand the challenges encountered by and demonstrate the capabilities of realistic attackers should they attempt to interfere with such systems as commonly deployed. In those years, Drew has built and demonstrated many proof-of-concept attacks across various areas of voting system security including Internet Voting, voter-facing software/hardware, ballot de-anonymization, and physical protections.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Do you feel in control? Analysis of AWS CloudControl API as an attack tool

Tags: Red Team Village | Misc

When: Sunday, Aug 9, 12:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 1 309 (Red Team Village) Tactic Table 1 - [Map](#)

Description:

"Identity is the new perimeter" gets thrown around a lot in security discussions, for a good reason. With the right privileges, cloud resources can be managed through APIs. Each provider has their own way of handling API access on resources. If your identity has the right permissions for a specific API call, you can execute that action.

The thing is, it's hard to remember every single API call you need to get specific information or access certain resources. AWS recognized this problem and created the AWS CloudControl API, a unified API that groups different resources together so you can create, update, delete, or retrieve them in bulk. This makes managing resources much simpler since you don't need to know which specific service, API call, or parameters to use.

But here's the catch: when something is easy for legitimate users, it's usually easy for attackers too. There are already tools available to use the AWS CloudControl API to pull resource information, and the technique is gaining attention.

But is it actually a good way to do stealthy enumeration? In this article, we examine what the CloudControl API is, how it simplifies resource management, how attackers can weaponize it, its limitations, and detection methods.

SpeakerBio: Bleon "gl4ssesbo1" Proko

Bleon is an Info-sec passionate about Infrastructure Penetration Testing and Security, including Active Directory, Cloud (AWS, Azure, GCP, Digital Ocean), Hybrid Infrastructures, as well as Defense, Detection and Thread Hunting. He has presented topics related to Cloud Penetration Testing and Security in conferences like BlackHat USA, Europe and Sector, DEF CON, SANS Pentest Hackfest Hollywood and Amsterdam, as well as several BSides on USA and Europe.

His research includes Nebula, a Cloud Penetration Testing Framework (<https://github.com/gl4ssesbo1/Nebula>) and other blogs, which you can also find on his blog (blog.pepperclipp.com). He is also the author of YetiHunter, DetentionDodger and Ransomwhen ([https://github.com/Permiso-io-tools/\[DetentionDodger|YetiHunter|Ransomwhen\]](https://github.com/Permiso-io-tools/[DetentionDodger|YetiHunter|Ransomwhen])).

He is also the author of the upcoming book "Deep Dive into Clouded Waters: An overview in Digital Ocean's Pentest and Security" (<https://leanpub.com/deep-dive-into-clouded-waters-an-overview-in-digitaloceans-pentest-and-security>)

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Misc - Saturday - 12:30-12:59 PDT

Title: Donating Bone Marrow: A Donor's First-Hand Experience

Tags: National Marrow Donor Program (Be the Match) | Creator Talk/Panel

When: Saturday, Aug 8, 12:30 - 12:59 PDT

Where: LVCCW Level 1 Hall 3 1100 (Creator Stage 7) - [Map](#)

Description:

Donating bone marrow can save lives, but many don't understand what it really involves. Find out the experience and how you can help participate in one of the coolest bio-hacks ever.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Contests - Saturday - 12:00-14:59 PDT

Title: Dozier Drill Tournament

Tags: Lockpick Village | Dozier Drill Lockpicking Challenge | Contest

When: Saturday, Aug 8, 12:00 - 14:59 PDT

Where: LVCCW Level 1 Hall 1 407 (Lockpick Village) - [Map](#)

Description:

Have you ever wanted to break out of handcuffs, pick open a closed bag and shoot your buddy in the chest with a nerf gun? So have we, that's why TOOOL presents the Dozier Drill. A fast paced skill based game where you have to free yourself from handcuffs, open a closed bag, and retrieve the nerf gun to be the first to hit the target. Join us on Friday for qualifiers, through the con for unofficial games, and on Saturday for an official bracket tournament.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: DPAPI Is Not a Boundary: A Full Infostealer Kill Chain Operators Can Replicate

Tags: Red Team Village | Misc

When: Saturday, Aug 8, 11:00 - 11:59 PDT

Where: LVCCW Level 1 Hall 1 309 (Red Team Village) Workshop Stage 1 - [Map](#)

Description:

Complete infostealer kill chain hands-on, executed against Windows 11 21H2 on default UAC using only open-source tooling. No zero-days, no commercial C2. Participants run every command live: HTA delivery, Meterpreter in-memory session, Chrome and Edge credential extraction via DPAPI-locked SQLite, keylogging in explorer.exe memory, UAC bypass via fodhelper, SYSTEM via Named Pipe Impersonation, and LSASS dump via Kiwi. The DPAPI_SYSTEM key recovered from LSA secrets decrypts the browser credentials captured earlier, closing the loop.

OUTLINE

Stage 1: generate HTA payload, deliver via Python HTTP server, open Meterpreter session Stage 2: extract Chrome and Edge credentials via post module, inspect DPAPI-encrypted loot Stage 3: migrate to explorer.exe, start keyscan, capture live keystrokes Stage 4: UAC bypass via fodhelper registry hijack, elevate to SYSTEM via Named Pipe Impersonation Stage 5: load Kiwi, dump NTLM hashes, SAM, LSA secrets, extract DPAPI_SYSTEM key, decrypt browser loot Detection debrief: Sysmon Event ID 1 process tree and PowerShell Script Block log review per stage

TAKEAWAYS

1. A complete credential theft playbook from HTA delivery to LSASS dump, validated against Windows 11 21H2 with Chrome 147 and Edge 147 on default UAC, ready to adapt for engagements.
2. The DPAPI close-loop: how DPAPI_SYSTEM from LSA secrets decrypts browser credentials collected earlier, giving operators a concrete credential pivot from a single user-context session.
3. A detection gap map calibrated against real Sysmon telemetry showing which events fire on default Windows 11 and which require EDR behavioral rules most organizations do not have deployed.

SpeakerBio: Filipi Pires, Head of Technical Advocacy at SCYTHE

I've been working as Head of Technical Advocacy at SCYTHE, Founder & Investor at CROSS-INTEL, Advisor & Investor at Sherlockeye, BSides Porto Organizer, Red Team Village Director (DEF CON), Senior Advisor Raices Cyber Academy, Founder of Red Team Community (Brazil and LATAM), AWS Community Builder, Snyk Ambassador, Application Security Specialist and Hacking is NOT a crime Advocate. International Speaker at Security and New technologies events in many countries such as US (Black Hat & Defcon), Canada, France, Spain, Germany, Poland, Black Hat MEA - Middle-East - and others, I've served as University Professor in Master Degree in Portugal, Graduation and MBA courses at Brazilian colleges, in addition, I'm Creator and Instructor of the Course - Malware Attack Types with Kill Chain Methodology (PentestMagazine), PowerShell and Windows for Red Teamers(PentestMagazine) and Malware Analysis - Fundamentals (HackerSec).

Black Hat US 2025 - <https://blackhat.com/us-25/arsenal/schedule/presenters.html#filipi-pires-46329> Black Hat US 2024 - <https://blackhat.com/us-24/arsenal/schedule/presenters.html#filipi-pires-46329> Black Hat MEA 2025 - <https://blackhatmea.com/speaker/filipi-pires-0> Black Hat MEA 2024 - <https://blackhatmea.com/speaker/filipi-pires> DEF CON 33 / 32 - <https://sessionize.com/filipi-pires/> DEF CON - Adversary Village - <https://adversaryvillage.org/adversary-events/DEFCON-33/Filipi-Pires/>



IoT Village - Friday - 12:30-13:15 PDT

Title: Dr. Strangepwn: How I Learned to Stop Worrying and Love the LLM

Tags: IoT Village | Creator Talk/Panel

When: Friday, Aug 7, 12:30 - 13:15 PDT

Where: LVCCW Level 1 Hall 3 1105 (Creator Stage 3) - [Map](#)

Description:

An AI agent found a previously undisclosed vulnerability in a named vendor's IoT product within hours of being pointed at the firmware. The practitioner who built the agent had spent 25+ years doing that work by hand. Plan R is an IoT-focused MCP server that gives AI agents direct access to real pentesting tools, structured by playbooks that encode methodology rather than scripts. The framework expanded from firmware-only analysis to a multi-domain suite covering WiFi, BLE, network protocols, and hardware interfaces, with each domain compounding the value of every other through cross-domain correlation. The centerpiece is a real engagement: a named vendor, a disclosed vulnerability, and the specific challenge of convincing a white box vendor that a finding is real when the methodology that found it is "an LLM read your code." Attendees leave with a working blueprint for building their own AI pentesting agents, an honest account of where the approach breaks, and a direct answer to the question every experienced practitioner is quietly asking: if an AI can do this, what exactly am I bringing to an engagement? The answer is worth hearing. But the work is changing, and this community should be driving how.

SpeakerBio: Larry Pesce

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Maritime Hacking Village - Friday - 13:45-14:15 PDT

Title: Drag, Drop, Deploy, Compromise: Why Trusted HMI Engineering Toolchains Remain an ICS Supply-Chain Blind Spot

Tags: Maritime Hacking Village | Creator Talk/Panel

When: Friday, Aug 7, 13:45 - 14:15 PDT

Where: LVCCW Level 1 Hall 3 801 (Creator Stage 2) - [Map](#)

Description:

HMI engineering tools are trusted gateways into industrial environments. Engineers use these tools to design screens, configure tags, connect to controllers, and deploy projects to real-world sites. HMIs are used across manufacturing, logistics, maritime, energy, utilities, building automation, and many other industrial sectors. Yet the engineering tools and project files used to create them are often treated as simple work utilities.

This presentation analyzes multiple vulnerabilities discovered in the HMI engineering toolchain from a supply chain perspective. It covers memory corruption during project file parsing, DLL search path hijacking, the loading of unsigned components, UI spoofing through silent font installation, and fallback to plaintext policies when secure OPC UA connections fail.

The core argument is simple: the ICS supply chain does not begin only at a vendor's update server. Project files received from customers, templates shared by system integrators, maintenance backups, local DLLs, fonts, communication settings, and the engineering workflow of "open, drag, and deploy" are all part of the supply chain.

This presentation shows that not only PLCs and HMI runtimes, but also the tools and files used to create them, are part of the attack surface.

Speakers: Jiwoon Yoo, TaeWoo Kim, Eunji choi

SpeakerBio: Jiwoon Yoo, CYTUR Inc

CYTUR Inc. / Security Team Lead

Research Areas and Interests Maritime Cybersecurity, Satellite Security, Large Language Models, Adversarial Attacks
Education and Professional Experience 2017: B.S. in Computer Science Engineering, Anyang University, Gyeonggi-do, South Korea 2023: M.S. in Convergence Security, Graduate School of Information Security, Korea University, Seoul, South Korea 2023 – Present: Security Team Lead, CYTUR Inc.

Academic Activities Symposium Participation * Nov 13–14, 2024: Participated in CFP-selected research at the IMO Maritime Cybersecurity Symposium (United Nations), London, UK

Journal Publication Sensors (May 24, 2023) — First author: Formulating Cybersecurity Requirements for Autonomous Ships Using the SQUARE Methodology <https://doi.org/10.3390/s23115033>

Sensors (Feb 26, 2022) — First author: Cyberattack Models for Ship Equipment Based on the MITRE ATT&CK Framework <https://doi.org/10.3390/s22051860>

SpeakerBio: TaeWoo Kim, CYTUR Inc

No BIO available

SpeakerBio: Eunji choi, CYTUR Inc

No BIO available



Game Hacking Village - Saturday - 16:00-16:59 PDT

Title: Dreamcast Ex Inferis — RCE on the Sega Dreamcast PlanetWeb Internet Browser v3.0

Tags: Game Hacking Village | Creator Talk/Panel

When: Saturday, Aug 8, 16:00 - 16:59 PDT

Where: LVCCW Level 1 Hall 1 211 (Game Hacking Village) - [Map](#)

Description:

SpeakerBio: Piffd0s

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Dreamcast Ex Inferis: RCE on the Sega Dreamcast PlanetWeb Browser

Tags: Game Hacking Village | Creator Talk/Panel

When: Saturday, Aug 8, 10:45 - 11:30 PDT

Where: LVCCW Level 1 Hall 3 801 (Creator Stage 2) - [Map](#)

Description:

The PlanetWeb Internet Browser v3.0 (2000–2001) is the official disc that let you browse the web and read email on a Dreamcast. Its online features depend on a backend server that no longer exists. The dreamcast is now a networked, code-downloading appliance whose trust model rests on a domain anyone can now point wherever they want.

What We Did

This is a full unauthenticated, network-only attack. By answering DNS for the dead backend domain, we get the browser to download and run our code. From there we chain through the mail client to reach the console's bare metal, and end by running DOOM natively.

No physical access, no modchip, no user trickery beyond opening one email. The console was built to download and trust code from a server that's gone — so we just become that server.

The talk walks through the chain at a high level, the obstacles of debugging a 24-year-old black box, and what it takes to get a modern game engine running in the few megabytes of RAM the Dreamcast has — ending with a live demo of DOOM running on the browser.

Why It Matters / Why It's Fun

It's a clean case study in why abandoned online infrastructure is a security problem that outlives the product, and it's a nostalgic hardware-hacking story with the most satisfying possible payoff: DOOM, on a Dreamcast, over the internet.

SpeakerBio: Christopher Hernandez, Binary Enthusiast

Chris Hernandez is a security researcher specializing in vulnerability discovery, exploitation, and large scale reverse engineering using IDA Pro. A Pwn2Own competitor in the ICS/SCADA and embedded systems categories, he actively collaborates with the reverse engineering community to solve binary analysis challenges.

--

Chris Hernandez is the founder of Adversary Consulting Group and an offensive security researcher with more than a decade of experience in vulnerability research, reverse engineering, and exploit development. He holds the OSEE certification and has competed at Pwn2Own in the IoT and ICS/SCADA categories.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Drive Stats: 14 years of hard drive failure rates

Tags: Data Duplication Village | Creator Talk/Panel

When: Saturday, Aug 8, 13:00 - 13:59 PDT

Where: LVCCW Level 2 W203 (Data Duplication Village) - [Map](#)

Description:

For over 14 years, Backblaze has been collecting the failure rates of hard drives in our data centers. But, what does that even mean? How do you define a failure, and how does that definition define or obscure the realities of drive performance?

SpeakerBio: Stephanie Doyle, Sr. Manager and Keeper of Stats at Backblaze

Stephanie Doyle is a Sr. Manager at Backblaze and known as the Keeper of Stats. She oversees the various first party data reports including Drive Stats, which reports on the failure rates of hard drives in Backblaze data centers; Network Stats, which reports on network traffic into and out of Backblaze's network; and Performance Stats, which publishes quarterly testing on cloud storage benchmarks. She specializes in taking complex topics and writing relatable, engaging, and user-friendly content. You can most often find her reading in public places, and can connect with her on LinkedIn.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Data Duplication Village - Friday - 11:00-11:59 PDT

Title: Drive Stats: 14 years of hard drive failure rates

Tags: Data Duplication Village | Creator Talk/Panel

When: Friday, Aug 7, 11:00 - 11:59 PDT

Where: LVCCW Level 2 W203 (Data Duplication Village) - [Map](#)

Description:

For over 14 years, Backblaze has been collecting the failure rates of hard drives in our data centers. But, what does that even mean? How do you define a failure, and how does that definition define or obscure the realities of drive performance?

SpeakerBio: Stephanie Doyle, Sr. Manager and Keeper of Stats at Backblaze

Stephanie Doyle is a Sr. Manager at Backblaze and known as the Keeper of Stats. She oversees the various first party data reports including Drive Stats, which reports on the failure rates of hard drives in Backblaze data centers; Network Stats, which reports on network traffic into and out of Backblaze's network; and Performance Stats, which publishes quarterly testing on cloud storage benchmarks. She specializes in taking complex topics and writing relatable, engaging, and user-friendly content. You can most often find her reading in public places, and can connect with her on LinkedIn.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Drogonsec: SAST + SCA + Secrets + IaC in one open-source scanner

Tags: AppSec Village | Creator Event/Activity | All Audiences

When: Friday, Aug 7, 12:45 - 13:45 PDT

Where: LVCCW Level 1 Hall 2 604 (Appsec Village) Arsenal - [Map](#)

Description:

Drogonsec is an open-source, high-performance security scanner built for developers and CI/CD pipelines. In a single run, it combines four analysis engines: SAST for 20+ languages, SCA for dependency CVEs, secret detection with 50+ patterns (AWS, GCP, GitHub, JWTs, SSH keys), and IaC misconfiguration analysis for Terraform and Kubernetes, all mapped to OWASP Top 10:2025 and CWE, with CVSS 3.1 scoring and SARIF output for GitHub and Azure DevOps integration.

This Arsenal session will demo Drogonsec scanning real-world repositories live, showing findings across all four engines, explaining rule design decisions, and showcasing how teams can extend it with custom YAML rules. Attendees leave with a running tool they can drop into their pipelines the same day.

SpeakerBio: Filipi Pires, Head of Technical Advocacy at SCYTHE

I've been working as Head of Technical Advocacy at SCYTHE, Founder & Investor at CROSS-INTEL, Advisor & Investor at Sherlockeye, BSides Porto Organizer, Red Team Village Director (DEF CON), Senior Advisor Raices Cyber Academy, Founder of Red Team Community (Brazil and LATAM), AWS Community Builder, Snyk Ambassador, Application Security Specialist and Hacking is NOT a crime Advocate. International Speaker at Security and New technologies events in many countries such as US (Black Hat & Defcon), Canada, France, Spain, Germany, Poland, Black Hat MEA - Middle-East - and others, I've served as University Professor in Master Degree in Portugal, Graduation and MBA courses at Brazilian colleges, in addition, I'm Creator and Instructor of the Course - Malware Attack Types with Kill Chain Methodology (PentestMagazine), PowerShell and Windows for Red Teamers(PentestMagazine) and Malware Analysis - Fundamentals (HackerSec).

Black Hat US 2025 - <https://blackhat.com/us-25/arsenal/schedule/presenters.html#filipi-pires-46329> Black Hat US 2024 - <https://blackhat.com/us-24/arsenal/schedule/presenters.html#filipi-pires-46329> Black Hat MEA 2025 - <https://blackhatmea.com/speaker/filipi-pires-0> Black Hat MEA 2024 - <https://blackhatmea.com/speaker/filipi-pires> DEF CON 33 / 32 - <https://sessionize.com/filipi-pires/> DEF CON - Adversary Village - <https://adversaryvillage.org/adversary-events/DEFCON-33/Filipi-Pires/>

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Aerospace Village - Friday - 10:00-17:59 PDT

Title: Drone Hacking Choose your Own Adventure

Tags: Aerospace Village | Creator Event/Activity

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 2 700 (Aerospace Village) - [Map](#)

Description:

Dive into our interactive choose-your-own-adventure web interface and learn how to hack a drone in a fun, storyboard-based game. This graphical user interface simulates the process we use when hacking drones for the Air Force, allowing participants to make decisions and see the outcomes.

It's a beginner-friendly, 15-30 minute activity offering insights into the steps involved in drone penetration testing.

Participants can access it from their own computers or mobile phones.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Aerospace Village - Sunday - 10:00-13:59 PDT

Title: Drone Hacking Choose your Own Adventure

Tags: Aerospace Village | Creator Event/Activity

When: Sunday, Aug 9, 10:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 2 700 (Aerospace Village) - [Map](#)

Description:

Dive into our interactive choose-your-own-adventure web interface and learn how to hack a drone in a fun, storyboard-based game. This graphical user interface simulates the process we use when hacking drones for the Air Force, allowing participants to make decisions and see the outcomes.

It's a beginner-friendly, 15-30 minute activity offering insights into the steps involved in drone penetration testing.

Participants can access it from their own computers or mobile phones.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Aerospace Village - Saturday - 10:00-17:59 PDT

Title: Drone Hacking Choose your Own Adventure

Tags: Aerospace Village | Creator Event/Activity

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 2 700 (Aerospace Village) - [Map](#)

Description:

Dive into our interactive choose-your-own-adventure web interface and learn how to hack a drone in a fun, storyboard-based game. This graphical user interface simulates the process we use when hacking drones for the Air Force, allowing participants to make decisions and see the outcomes.

It's a beginner-friendly, 15-30 minute activity offering insights into the steps involved in drone penetration testing.

Participants can access it from their own computers or mobile phones.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Aerospace Village - Friday - 10:00-17:59 PDT

Title: Drone Hacking Workshop

Tags: Aerospace Village | Creator Event/Activity

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 2 700 (Aerospace Village) - [Map](#)

Description:

Join our Drone Hacking Workshop for hands-on experience hacking drone components. This three-step in-depth activity is designed to teach you about the vulnerabilities and security of autonomous systems. Using sample drones, participants will learn techniques used in government pen tests.

This 2-3 hour workshop suits all skill levels, from beginners to advanced hackers. Come and test your skills in a real-world scenario and understand the intricacies of drone security.

Participants need to bring a laptop capable of running a Linux distribution.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Aerospace Village - Saturday - 10:00-17:59 PDT

Title: Drone Hacking Workshop

Tags: Aerospace Village | Creator Event/Activity

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 2 700 (Aerospace Village) - [Map](#)

Description:

Join our Drone Hacking Workshop for hands-on experience hacking drone components. This three-step in-depth activity is designed to teach you about the vulnerabilities and security of autonomous systems. Using sample drones, participants will learn techniques used in government pen tests.

This 2-3 hour workshop suits all skill levels, from beginners to advanced hackers. Come and test your skills in a real-world scenario and understand the intricacies of drone security.

Participants need to bring a laptop capable of running a Linux distribution.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Aerospace Village - Sunday - 10:00-13:59 PDT

Title: Drone Hacking Workshop

Tags: Aerospace Village | Creator Event/Activity

When: Sunday, Aug 9, 10:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 2 700 (Aerospace Village) - [Map](#)

Description:

Join our Drone Hacking Workshop for hands-on experience hacking drone components. This three-step in-depth activity is designed to teach you about the vulnerabilities and security of autonomous systems. Using sample drones, participants will learn techniques used in government pen tests.

This 2-3 hour workshop suits all skill levels, from beginners to advanced hackers. Come and test your skills in a real-world scenario and understand the intricacies of drone security.

Participants need to bring a laptop capable of running a Linux distribution.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Drone ID on the Wire: RF Detection, Spoofing, and the Limits of Compliance-Based Airspace Awareness

Tags: Radio Frequency Village | Creator Talk/Panel

When: Saturday, Aug 8, 15:00 - 15:55 PDT

Where: LVCCW Level 1 Hall 1 409 (Radio Frequency Village) - [Map](#)

Description:

The low-altitude airspace has an RF problem. The FAA mandated Remote ID as the foundational identification standard for drone operations across the United States - a broadcast protocol running on Bluetooth and WiFi that any phone is supposed to receive. The problem is that it was designed for individual accountability, not area surveillance, has a practical detection range measured in hundreds of meters, is completely unencrypted and unauthenticated, and is trivially spoofable with an ESP8266 and three dollars in hardware. Meanwhile the proprietary protocol it largely replaced - DJI's OcuSync Drone ID - was detectable at tens of kilometers, is now encrypted on newer hardware, and its primary detection product was discontinued. The gap between what practitioners think Remote ID provides and what it actually provides is a fundamental RF problem with direct public safety consequences.

This talk lives in the RF layer. We will cover what drone broadcasts actually look like on a receiver - Remote ID over BLE advertising channels 37/38/39 and WiFi beacon frames on channels 6 and 149, DJI Drone ID embedded in OcuSync, and what non-broadcasting drones look like (nothing). We will walk through the full detection stack from a \$50 COTS build (Ubiquiti Bullet M2, OpenWRT, tcpdump, Wireshark, OpenDroneID dissector) through man-portable dedicated receivers (DroneTag Rider), distributed mobile detection via ATAK plugins (Drone Hone), and enterprise fixed-site systems - and we will show real sensor performance data from multi-sensor deployments at major federal security operations. Key finding: 95.5% of unique drones detected across a SEAR 1 National Special Security Event were seen by only a single sensor. The multi-sensor fusion problem is unsolved at urban scale, and the urban RF environment - path loss, noise floor, building shadows — is why. We will then walk through the spoofing ecosystem in depth. Ghost swarm attacks (jjshoots/RemoteIDSpoofer - 16 fake drones, web UI, \$3 ESP8266), pilot location spoofing (brinuk/Remote-ID-Drone-and-Pilot-Spoofers - sends ground teams to empty parking lots), DJI Drone ID spoofing (DJISDKUser/ESP8266_DJI_DroneID_Throwie - Kevin Finisterre, taped to a fence, runs forever), and protocol-level implementations (cyber-defence-campus/droneRemoteIDSpoofer - Python/Scapy, ASTM F3411 plus DJI format, Swiss Cyber Defence Campus provenance). All public, all GitHub, all under \$5 hardware. We will cover the attack taxonomy: evasion, flooding, identity spoofing, and operator location spoofing - and what each one means operationally for the detection stack.

The legal layer is real and the audience should know it: 6 USC 124n authorizes four federal agencies to take action against drones. Nobody else can jam, spoof, or kinetically defeat without federal authority. The possession/testing/broadcasting distinction matters and we will be clear about it.

We close with the governance gap: Remote ID's authentication-free design was a deliberate policy choice. The FAA Reauthorization Act of 2024 directed a review of whether cryptographic signing could be added. That review is ongoing. The people in this room build the tools that inform these conversations - this is the right audience to have opinions about what the answer should be.

No policy background required. If you know what a waterfall is you are the target audience.

SpeakerBio: Greg Albrecht

No BIO available

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Aerospace Village - Friday - 15:00-15:30 PDT

Title: Drones, Detectors, and the Kill Chain

Tags: Aerospace Village | Creator Talk/Panel

When: Friday, Aug 7, 15:00 - 15:30 PDT

Where: LVCCW Level 1 Hall 3 1103 (Creator Stage 5) - [Map](#)

Description:

Counter-Unmanned Aircraft Systems (C-UAS) is a domain spanning RF engineering, federal law, operational security, and public policy, and it's being built right now by people working without a complete picture. Most security practitioners and nearly all civilians don't know how drone detection works, what the legal framework for defeating drones is, who's authorized to do what and why, or how badly the current technical stack can be defeated with a microcontroller. Drawing on direct operational experience at SEAR 1 National Special Security Events (the highest domestic security classification in the United States), this presentation walks through the complete C-UAS stack from first principles, grounded in real operational data rather than vendor marketing.

SpeakerBio: Greg Albrecht

No BIO available

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Dylib Hijacking on macOS: Dead or Alive?

Tags: DEF CON Official Talk | Demo

When: Saturday, Aug 8, 13:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 3 906 (Main Track 3) - [Map](#)

Description:

Over a decade ago, a much younger Patrick showed that macOS (then OS X) was vulnerable to what had long been considered a Windows-only attack: dynamic library hijacking. By planting malicious libraries in the right place, attackers could achieve stealthy persistence, inject code into trusted processes, and even bypass core Apple security mechanisms.

Today, an older (and hopefully wiser) Patrick revisits that work to answer a simple question: is dylib hijacking truly dead on modern macOS, or has Apple's decade of defenses, including Gatekeeper, App Translocation, Notarization, and the Hardened Runtime, simply made it harder?

This talk revisits the technique in 2026, analyzing these mitigations and evaluating their real-world effectiveness. While the attack surface has been significantly reduced, we show dylib hijacking remains possible under the right conditions. Through real-world examples and live demos, we explore how modern applications can still be coerced into loading attacker-controlled libraries, enabling code execution within trusted processes and bypassing controls such as TCC.

Finally, we present practical detection and defense strategies, including novel approaches leveraging Endpoint Security to detect (and block!) malicious library loads at runtime.

"Dylib hijacking on OS X" ” www.virusbulletin.com/virusbulletin/2015/03/dylib-hijacking-os-x

"Tweaking macOS security controls to thwart application bundle manipulation"
” redcanary.com/blog/threat-detection/mac-application-bundles/

"What's New in Security" (WWDC 2016)”
devstreaming-cdn.apple.com/videos/wwdc/2016/706sgjvzkvg6rrg9icw/706/706_whats_new_in_security.pdf

SpeakerBio: Patrick Wardle, CEO and Co-Founder at DoubleYou

Patrick Wardle is the cofounder of the Objective-See Foundation, CEO and cofounder of DoubleYou, and author of The Art of Mac Malware series. He previously worked at NASA and the NSA, and has presented at countless security conferences, making him intimately familiar with aliens, spies, and talking nerdy.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Bug Bounty Village - Saturday - 12:30-12:59 PDT

Title: Eating Our Own Dogfood: Running a Bug Bounty Program on a Bug Bounty Platform

Tags: Bug Bounty Village | Creator Talk/Panel

When: Saturday, Aug 8, 12:30 - 12:59 PDT

Where: LVCCW Level 1 Hall 3 1102 (Creator Stage 6) - [Map](#)

Description:

At HackerOne, the same community that submits vulnerability reports also tests the platform they use to report them. Every report becomes a live stress test of our product, workflows, assumptions, and newly shipped features. In this talk, a Senior Triage Lead and a Product Security Engineer share what we learned from running HackerOne's own bug bounty program while shipping GraphQL features, AI-assisted tooling, disclosure workflows, and platform-scale infrastructure changes. Using three real disclosed reports, we walk through how seemingly small bugs escalated into platform-wide security lessons: 1. An Elasticsearch query parameter that enabled metadata enumeration through raw script execution. 2. A PDF export feature that unintentionally exposed internal triage activity. 3. An AI agent that exposed non-public report metadata because a researcher asked the right question. We will show how reports move from submission to validation, severity debates, engineering response, remediation, retesting, and disclosure. We will also discuss how we use our own program as a testing ground for AI-assisted triage, automated validation workflows, and disclosure policies before rolling changes out more broadly. This is not a "how to run a bug bounty program" talk. It is a behind-the-scenes look at what happens when hackers continuously attack the bug bounty platform itself and how that pressure forces rapid security evolution. Attendees will leave with practical lessons on: 1. building tighter triage-to-engineering feedback loops, 2. handling modern attack surfaces like GraphQL and AI agents, 3. scaling remediation without losing researcher trust, 4. and turning bug bounty programs into product improvement engines instead of passive inboxes. All case studies are based on disclosed HackerOne reports. No customer data was accessed or exposed.

Speakers: Shrimant Subhash More, Martzen Haagsma

SpeakerBio: Shrimant Subhash More, Senior Security Analyst, HackerOne

Shrimant Subhash More is a Senior Product Security Analyst at HackerOne with over 8 years of experience in offensive security, penetration testing, and vulnerability management. His expertise spans web, API, mobile (Android and iOS), and AI/LLM security, with more than 300 security assessments conducted across diverse industry sectors. At HackerOne, Shrimant leads and supports vulnerability triage operations, validates security reports submitted by researchers, handles escalations, mentors analysts, and collaborates with global teams to improve security outcomes and triage efficiency. He is passionate about offensive security, product security operations, security automation, and helping organizations build resilient products. Beyond his professional role, Shrimant actively contributes to the cybersecurity community as a HackerOne Community Brand Ambassador for India West (Pune), where he organizes meetups, conducts workshops, mentors aspiring researchers, and promotes responsible disclosure and bug bounty programs. He is the assignee of CVE-2020-35296 and holds multiple industry certifications across security, cloud, and AI domains.

SpeakerBio: Martzen Haagsma, Security Engineer, HackerOne

Martzen Haagsma is a Product Security Engineer at HackerOne with a passion for building secure systems through collaboration, automation, and continuous learning. With experience spanning security testing, DevOps engineering, and technical leadership, Martzen focuses on helping organizations identify vulnerabilities, improve security processes, and strengthen their overall security posture. Known for a solution-oriented mindset and a strong belief in the power of teamwork, Martzen enjoys connecting people, sharing knowledge, and turning complex security challenges into practical outcomes. Prior to joining HackerOne, Martzen worked across both public and private sectors in roles involving security testing, agile quality engineering, and engineering leadership. Outside of work, Martzen is an active technologist with interests ranging from security and software development to automation, IoT, and 3D printing. Through writing, mentoring, and community engagement, Martzen advocates for curiosity, collaboration, and making technology more secure and accessible for everyone.



Contests - Saturday - 18:00-20:59 PDT

Title: EFF Tech Trivia

Tags: EFF Tech Trivia | Contest

When: Saturday, Aug 8, 18:00 - 20:59 PDT

Where: LVCCW Level 1 Hall 1 100 (Contest Stage) - [Map](#)

Description:

EFF's privacy and security experts have crafted a new trivia challenge for DEF CON 34! Compete as a team in our no-holds-barred showdown to prove mastery over the obscure facts of digital security, online rights, and internet culture.

The First Place team wins a set of custom Cybertiger Champion Badges and EFF swag. Second and third place teams will also win Badges and EFF gear.

Invite your friends OR show up and make new friends! Did someone say BRIBES? The world is unfair! You too could influence the judges to add a point or two to your team's tally. Overall Bribe winner also wins a custom badge! Test your knowledge of all things tech and support EFF, too.

Participant Prerequisites

No phones, laptops, or other digital knowledge allowed! Just you, your friends, and a friendly game of trivia.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: El regreso de Sedinho: situación actual y nuevas tácticas de los troyanos bancarios brasileños

Tags: La Villa Community | Creator Talk/Panel

When: Friday, Aug 7, 15:00 - 15:30 PDT

Where: LVCCW Level 1 Hall 4 1416 (La Villa Community) Main Stage - [Map](#)

Description:

Esta investigación analiza la evolución reciente de los troyanos bancarios brasileños y su expansión internacional, así como las acciones de las autoridades para frenarlos. Se examinan campañas actuales impulsadas por ciberdelincuentes latinoamericanos que no solo perfeccionan el malware bancario tradicional, sino que también incorporan fraudes móviles basados en tecnología NFC.

SpeakerBio: Josep Albors, Head of Awareness & Research at Ontinet.com (ESET Spain)

Josep Albors is the Head of Awareness & Research at Ontinet.com (ESET Spain). He's a security expert with more than 21 years working in cybersecurity and specialized in security awareness. He is also the editor at the company's blog and one of the experts writing at several other publications related with the IT security world in Spain.

He has been a speaker at some of the most important security conferences in Spain, besides collaborating with initiatives such as X1RedMasSegura, that wants to raise awareness among users so they can use Internet and technology in a safe way. Included in Ontinet's social responsibility, Josep also does awareness and cybersecurity presentations in schools and universities. He's also a teacher in cyber security expert courses at several Spanish Universities and participates in several conferences organized by several spanish universities and Spain's national Institute of Cyber Security. He also participated as speaker at AVAR conference in Osaka in 2019, Caro Workshop 2023 in Bochum (Germany), FIRST 2024 (Fukuoka), Virus Bulletin 2024 (Dublín), Defcon Malware Village (2025), JSAC 2025 (Tokyo) and CARO 2026 (Innsbruck).

Josep has also collaborated with the Spanish Guardia Civil, Spanish National Police and the Spanish Army, teaching their units on how to fight cybercrime and with cyber intelligence training, contributing with his experience in analyzing cybercrime and malware.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Voting Village - Friday - 10:00-10:30 PDT

Title: Election Integrity and Technology

Tags: Voting Village | Creator Talk/Panel

When: Friday, Aug 7, 10:00 - 10:30 PDT

Where: LVCCW Level 2 W220 (Voting Village) (Voting Village Talks) - [Map](#)

Description:

This talk will give an overview of the technology used in US elections, the security vulnerabilities that can compromise elections, and approaches for making elections more secure and robust.

SpeakerBio: Matt Blaze

Matt Blaze is the McDevitt chair in Computer Science and Law at Georgetown University, where he studies problems at the intersection of technology and public policy. Election systems and voting technology are central focuses of his research. He led teams as part of the California TTBR and Ohio EVEREST studies that each found deep and fundamental weaknesses in different election technologies used by those states and the rest of the US. He has testified on technical risks in elections before the US Congress and other bodies numerous times. Blaze is a co-founder of the Voting Village and president of the Election Integrity Foundation.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Election Observation: Watching is not Enough

Tags: Voting Village | Creator Talk/Panel

When: Saturday, Aug 8, 17:00 - 17:30 PDT

Where: LVCCW Level 2 W220 (Voting Village) (Voting Village Talks) - [Map](#)

Description:

As Dan Wallach once said, an election must convince the losers that they lost fair and square. To do this, election administrators need to do more than merely allowing observers from all parties to watch, we must ensure that observers can understand what they are seeing. Watching the back of an election administrator doing something with a computer or even a with a stack of papers is not useful. Anecdotal reports by observers can give a feel for how an election was conducted, but systematic and well documented reporting is far more powerful. Election observation is difficult with simple in-person vote-for one contests; vote by mail, Internet voting and instant runoff voting all pose serious problems for election observers. We must demand electoral procedures that are easy to understand, and we must demand public documentation of those procedures. This talk will focus on successes and failures in election observation and suggest directions for future improvement.

SpeakerBio: Douglas W. Jones

Douglas W. Jones has been involved with election technology since he was appointed to the Iowa Board of Examiners for Voting Machines and Electronic Voting Systems in 1994. Since then, contributed to the 2002 FEC Voting System Standards, served on the Election Assistance Commission's Technical Guidelines Development Committee, tested voting equipment in Miami and Phoenix, and observed elections in Kazakhstan and the Netherlands. He has testified about voting technology before the House Science Committee, the Federal Election Commission, and in numerous court cases. He was a principal investigator in the NSF funded ACCURATE project, and with Barbara Simons, co-authored the book Broken (CSLI Press, 2012).

He got his PhD in Computer Science from the University of Illinois in 1980, and was on the CS University of Iowa CS faculty until 2021. These days, when he is not answering questions about elections, he is working with a small group of students to restore a 1965-vintage PDP-8 computer.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Election Security in the Age of AI: Governance, Trust, and the Systems Behind Democracy

Tags: Policy @ DEF CON | Creator Talk/Panel

When: Friday, Aug 7, 12:00 - 12:59 PDT

Where: LVCCW Level 2 W210-211 (Policy Village) - [Map](#)

Description:

Election security is often framed as a technology problem. In reality, it's a governance problem operating inside a highly stressed public system. This session brings together leaders who were inside that system during the most scrutinized election cycles in modern U.S. history, moderated by an elections policy expert who has shaped how platforms handle political content at global scale. Tim Harper, Project Lead for Elections and Democracy at the Center for Technology and Democracy and former Content Policy Associate Manager for Political Advertising at Meta, will moderate. His work focuses on combating election disinformation, strengthening election integrity, and building public trust. Lester Godsey served as CISO for Maricopa County during the 2020 and 2024 presidential elections, leading cybersecurity in a jurisdiction under intense national scrutiny and multiple adversaries. Bill Gates served on the Maricopa County Board of Supervisors during that same period, overseeing election administration amid unprecedented political pressure, misinformation and reputational and physical threats. He now directs the Mechanics for Democracy Laboratory at Arizona State University. Together, they bring a rare perspective: cybersecurity, governance, and systems engineering at the front lines of democracy.

Speakers: Lester Godsey, William Gates, Tim Harper

SpeakerBio: Lester Godsey, Arizona State University

Lester Godsey serves as the Chief Information Security Officer (CISO) for Arizona State University, the largest public university by enrollment in the United States. His appointment follows a distinguished five-year tenure as CISO for Maricopa County, where he skillfully managed information security during one of the most contentious election periods in the county's modern history. With over 30 years of public-sector IT experience, Lester is a respected voice in the field, having presented at local, state, and national levels on a diverse range of topics including telecommunications, data management, and cybersecurity. A lifelong learner and educator, Lester holds multiple industry certifications including PMP, CISM, and CISSP. He has shared his expertise as a collegiate instructor for almost fifteen years, teaching cybersecurity, technology, and project management courses. Lester is also a published author and actively contributes to the cybersecurity community. His academic background uniquely blends the arts and technology, holding both a Bachelor of Arts in Music and a Master of Science in Technology from Arizona State University. This multidisciplinary foundation informs his innovative approach to information security leadership.

SpeakerBio: William Gates, Arizona State University

Bill Gates is Executive Director of the ASU Mechanics of Democracy Laboratory (MODL) and Professor of Practice at Arizona State University's Watts College of Public Service and Community Solutions. He leads MODL's efforts to professionalize election administration through practitioner-focused training, transparency initiatives, and the integration of emerging technologies. In 2025, he launched the AI + Elections Clinic to equip election officials nationwide with the tools and expertise to responsibly harness artificial intelligence in support of voter confidence and election integrity.

Bill previously served two terms on the Maricopa County Board of Supervisors (2017–2024), overseeing elections in one of the nation's largest voting jurisdictions during the highly scrutinized 2020 and 2022 election cycles. He also served on the Phoenix City Council (2009–2016), including as Vice Mayor.

Bill is the recipient of various awards, commending his years of leadership, service, and defense of democracy including The American Bar Association's Unsung Hero of Democracy Award in 2024, The Truman Foundation's Joseph E. Stevens Public Service Award in 2022, The Arizona Republic's 2021 Arizonan of the Year, and The Phoenix Business Journal's Forty Under

SpeakerBio: Tim Harper, Center for Technology and Democracy

Tim Harper is Project Lead for Elections and Democracy, where he leads efforts to combat election disinformation, support secure voting technologies, and strengthen public trust in elections. An elections policy expert, Tim has driven policy and advocacy across industry and civil society. Most recently, he served as Content Policy Associate Manager for Political Advertising at Meta, where he developed and implemented global policies governing electoral, political, and social issue advertising. His work focused on transparency, preventing foreign interference, and countering election delegitimization at scale. Previously, Tim was Senior Elections Policy Analyst at the Bipartisan Policy Center, where he led election administration policy development and federal and state advocacy efforts. He convened a bipartisan task force of election officials to inform policymaking and led major data-driven research initiatives, including the largest national study on voting line disparities. He began his career supporting election management bodies in the Middle East and North Africa with the International Foundation for Electoral Systems. He graduated magna cum laude from Gonzaga University with degrees in Political Science and History.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Embedded Systems Village - Friday - 10:00-17:59 PDT

Title: Embedded - 101 Labs

Tags: Embedded Systems Village | Creator Event/Activity

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 2 503 (Embedded Systems Village) - [Map](#)

Description:

We have a lab platform that brings everyone from every skill level to the same playing field with step by step instructions that aim to teach individuals specific techniques and skills in a hands-on manner on embedded hacking techniques.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Embedded Systems Village - Saturday - 10:00-17:59 PDT

Title: Embedded - 101 Labs

Tags: Embedded Systems Village | Creator Event/Activity

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 2 503 (Embedded Systems Village) - [Map](#)

Description:

We have a lab platform that brings everyone from every skill level to the same playing field with step by step instructions that aim to teach individuals specific techniques and skills in a hands-on manner on embedded hacking techniques.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Embedded Systems Village - Sunday - 10:00-13:59 PDT

Title: Embedded - 101 Labs

Tags: Embedded Systems Village | Creator Event/Activity

When: Sunday, Aug 9, 10:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 2 503 (Embedded Systems Village) - [Map](#)

Description:

We have a lab platform that brings everyone from every skill level to the same playing field with step by step instructions that aim to teach individuals specific techniques and skills in a hands-on manner on embedded hacking techniques.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Embedded & Shredded: Advanced Embedded System Hacking

Tags: Biohacking Village | Creator Event/Activity

When: Sunday, Aug 9, 10:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 1 408 (Biohacking Village) - [Map](#)

Description:

This course offers a deep dive into practical techniques for dissecting and manipulating embedded systems. Get hands-on with these core activities:

- Visually inspect and document a device to map components, debug interfaces, and attack surfaces
- Decode board communication protocols with logic analyzers
- Exfiltrate live data over SPI, JTAG, and SWD — and use chip-off / deadbugging to reach embedded storage
- Reverse-engineer bare-metal firmware in Ghidra with advanced plugins
- Probe embedded defenses — encryption, disabled debug interfaces, glitching, and fault injection
- Chain hardware-level access into higher-level exploits — from physical interfaces all the way up to network-exposed services

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Biohacking Village - Friday - 10:00-17:59 PDT

Title: Embedded & Shredded: Advanced Embedded System Hacking

Tags: Biohacking Village | Creator Event/Activity

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 408 (Biohacking Village) - [Map](#)

Description:

This course offers a deep dive into practical techniques for dissecting and manipulating embedded systems. Get hands-on with these core activities:

- Visually inspect and document a device to map components, debug interfaces, and attack surfaces
- Decode board communication protocols with logic analyzers
- Exfiltrate live data over SPI, JTAG, and SWD — and use chip-off / deadbugging to reach embedded storage
- Reverse-engineer bare-metal firmware in Ghidra with advanced plugins
- Probe embedded defenses — encryption, disabled debug interfaces, glitching, and fault injection
- Chain hardware-level access into higher-level exploits — from physical interfaces all the way up to network-exposed services

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Embedded & Shredded: Advanced Embedded System Hacking

Tags: Biohacking Village | Creator Event/Activity

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 408 (Biohacking Village) - [Map](#)

Description:

This course offers a deep dive into practical techniques for dissecting and manipulating embedded systems. Get hands-on with these core activities:

- Visually inspect and document a device to map components, debug interfaces, and attack surfaces
- Decode board communication protocols with logic analyzers
- Exfiltrate live data over SPI, JTAG, and SWD — and use chip-off / deadbugging to reach embedded storage
- Reverse-engineer bare-metal firmware in Ghidra with advanced plugins
- Probe embedded defenses — encryption, disabled debug interfaces, glitching, and fault injection
- Chain hardware-level access into higher-level exploits — from physical interfaces all the way up to network-exposed services

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

The Diana Initiative - Saturday - 11:30-11:40 PDT

Title: Embedded System Village Tour

Tags: The Diana Initiative | Creator Tour

When: Saturday, Aug 8, 11:30 - 11:40 PDT

Where: LVCCW Level 1 South Lobby / Atrium - [Map](#)

Description:

Interested in visiting Embedded System Village but afraid to go by yourself? The Diana Initiative is hosting tours! Follow a volunteer to Embedded System Village and be introduced to the community and activities inside!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Embedded Systems Village - Saturday - 10:00-17:59 PDT

Title: Embedded Systems Village CTF

Tags: Embedded Systems Village | Creator Event/Activity

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 2 503 (Embedded Systems Village) - [Map](#)

Description:

Get hands-on with devices you won't find anywhere else — rare, hard-to-source embedded devices staged for live exploitation. Hunt real zero-days, and yes, bring your AI: LLM-assisted tooling is fully allowed, so use it to go as deep as you can.

Come break something that's never been broken.

New to embedded? Just wrapped our 101 Labs? Beginner challenges are available as well to apply your new found knowledge!

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Embedded Systems Village - Friday - 10:00-17:59 PDT

Title: Embedded Systems Village CTF

Tags: Embedded Systems Village | Creator Event/Activity

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 2 503 (Embedded Systems Village) - [Map](#)

Description:

Get hands-on with devices you won't find anywhere else — rare, hard-to-source embedded devices staged for live exploitation. Hunt real zero-days, and yes, bring your AI: LLM-assisted tooling is fully allowed, so use it to go as deep as you can.

Come break something that's never been broken.

New to embedded? Just wrapped our 101 Labs? Beginner challenges are available as well to apply your new found knowledge!

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Embedded Systems Village - Sunday - 10:00-13:59 PDT

Title: Embedded Systems Village CTF

Tags: Embedded Systems Village | Creator Event/Activity

When: Sunday, Aug 9, 10:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 2 503 (Embedded Systems Village) - [Map](#)

Description:

Get hands-on with devices you won't find anywhere else — rare, hard-to-source embedded devices staged for live exploitation. Hunt real zero-days, and yes, bring your AI: LLM-assisted tooling is fully allowed, so use it to go as deep as you can.

Come break something that's never been broken.

New to embedded? Just wrapped our 101 Labs? Beginner challenges are available as well to apply your new found knowledge!

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Empire 7: Shipping a C2 at AI Speed

Tags: Intro/Beginner | AI | DEF CON Demo Labs | DevOps | Malware | Offense/Red Team | Purple Team | DEF CON Demo Labs

When: Saturday, Aug 8, 12:00 - 12:45 PDT

Where: LVCCW Level 1 Hall 3 902 (Demo Labs Track 6) - [Map](#)

Description:

Empire 7 is a near-total overhaul of the Command and Control (C2) framework, from how agents communicate with the server to how operators move through engagements. This major release continues to expand Empire's supported agents to include PowerShell, Python, IronPython, Go, C#, and now C. New tradecraft includes more than 50 new modules derived from Atomic Red Team, patchless AMSI/ETW bypasses, EarlyBird process hollowing, BOF execution with ILRepack assembly merging, and RDP session hijacking, among others. Empire's new cryptographically secure communications leverage AES-256-GCM and mTLS, with MITRE ATT&CK integration to assist in emulating real-world Advanced Persistent Threat (APT) Tactics, Techniques, and Procedures (TTPs).

One more thing we'll talk about, this release shipped at roughly 10x our prior pace, due to our team's adoption of agentic coding tools as a core development collaborator. We'll share what worked, what didn't, and what LLM-assisted offensive tooling development looks like.

Speakers: Vincent "Vinnybod" Rose, Jake "Hubbl3" Krasnov, Anthony "Coin" Rose

SpeakerBio: Vincent "Vinnybod" Rose

Vincent "Vinnybod" Rose is the Lead Developer for Empire and Starkiller. He is a software engineer with a decade of expertise in building highly scalable cloud services, improving developer operations, and automation. Recently, his focus has been on the reliability and stability of the Empire C2 server. Vinnybod has presented at Black Hat and has taught courses at DEF CON on Red Teaming and Offensive PowerShell. He currently maintains a cybersecurity blog focused on offensive security at <https://bcsecurity.io/blog/>.

SpeakerBio: Jake "Hubbl3" Krasnov

Jake "Hubble" Krasnov is the Red Team Operations Lead at BC Security, with a distinguished career spanning engineering and cybersecurity. A U.S. Air Force veteran, Jake began his career as an Astronautical Engineer overseeing rocket modifications, leading test and evaluation efforts for the F-22, and conducting red team operations with the 57th Information Aggressors. He later served as a Technical Lead Engineer at Boeing Phantom Works, where he focused on embedded security for aviation and space defense projects. A seasoned speaker and trainer, Jake has presented at DEF CON, Black Hat, HackRedCon, HackSpaceCon, and HackMiami, and has previously taught Empire and offensive PowerShell at DEF CON.

SpeakerBio: Anthony "Coin" Rose

Dr. Anthony "Coin" Rose is an officer in the United States Air Force, an Assistant Professor, and the Director of the Center for Cyberspace Research at the Air Force Institute of Technology. He holds a doctorate in Electrical Engineering and has expertise in machine learning, with a focus on its application to cybersecurity and malware detection. He is also the founder of SIMAPTIC and the Director of Security Research at BC Security, where he specializes in adversary tactics and emulation planning, Red and Blue Team operations, and embedded systems security. Dr. Rose is credited with 16 CVEs and has presented at numerous security conferences, including Black Hat, DEF CON, HackSpaceCon, HackMiami, and RSA Conference.



Title: Empire 7: Shipping a C2 at AI Speed

Tags: Intro/Beginner | AI | DEF CON Demo Labs | DevOps | Malware | Offense/Red Team | Purple Team | DEF CON Demo Labs

When: Friday, Aug 7, 10:00 - 10:45 PDT

Where: LVCCW Level 1 Hall 3 902 (Demo Labs Track 6) - [Map](#)

Description:

Empire 7 is a near-total overhaul of the Command and Control (C2) framework, from how agents communicate with the server to how operators move through engagements. This major release continues to expand Empire's supported agents to include PowerShell, Python, IronPython, Go, C#, and now C. New tradecraft includes more than 50 new modules derived from Atomic Red Team, patchless AMSI/ETW bypasses, EarlyBird process hollowing, BOF execution with ILRepack assembly merging, and RDP session hijacking, among others. Empire's new cryptographically secure communications leverage AES-256-GCM and mTLS, with MITRE ATT&CK integration to assist in emulating real-world Advanced Persistent Threat (APT) Tactics, Techniques, and Procedures (TTPs).

One more thing we'll talk about, this release shipped at roughly 10x our prior pace, due to our team's adoption of agentic coding tools as a core development collaborator. We'll share what worked, what didn't, and what LLM-assisted offensive tooling development looks like.

Speakers: Vincent "Vinnybod" Rose, Jake "Hubbl3" Krasnov, Anthony "Coin" Rose

SpeakerBio: Vincent "Vinnybod" Rose

Vincent "Vinnybod" Rose is the Lead Developer for Empire and Starkiller. He is a software engineer with a decade of expertise in building highly scalable cloud services, improving developer operations, and automation. Recently, his focus has been on the reliability and stability of the Empire C2 server. Vinnybod has presented at Black Hat and has taught courses at DEF CON on Red Teaming and Offensive PowerShell. He currently maintains a cybersecurity blog focused on offensive security at <https://bcsecurity.io/blog/>.

SpeakerBio: Jake "Hubbl3" Krasnov

Jake "Hubble" Krasnov is the Red Team Operations Lead at BC Security, with a distinguished career spanning engineering and cybersecurity. A U.S. Air Force veteran, Jake began his career as an Astronautical Engineer overseeing rocket modifications, leading test and evaluation efforts for the F-22, and conducting red team operations with the 57th Information Aggressors. He later served as a Technical Lead Engineer at Boeing Phantom Works, where he focused on embedded security for aviation and space defense projects. A seasoned speaker and trainer, Jake has presented at DEF CON, Black Hat, HackRedCon, HackSpaceCon, and HackMiami, and has previously taught Empire and offensive PowerShell at DEF CON.

SpeakerBio: Anthony "Coin" Rose

Dr. Anthony "Coin" Rose is an officer in the United States Air Force, an Assistant Professor, and the Director of the Center for Cyberspace Research at the Air Force Institute of Technology. He holds a doctorate in Electrical Engineering and has expertise in machine learning, with a focus on its application to cybersecurity and malware detection. He is also the founder of SIMAPTIC and the Director of Security Research at BC Security, where he specializes in adversary tactics and emulation planning, Red and Blue Team operations, and embedded systems security. Dr. Rose is credited with 16 CVEs and has presented at numerous security conferences, including Black Hat, DEF CON, HackSpaceCon, HackMiami, and RSA Conference.



Title: Emulating the “Identity-First” Threat Actor: Automated Playbooks for IdP Hijacking

Tags: Adversary Village | Creator Talk/Panel

When: Saturday, Aug 8, 10:30 - 10:59 PDT

Where: LVCCW Level 1 Hall 3 1105 (Creator Stage 3) - [Map](#)

Description:

Modern intrusions often start with identity, not malware. Adversaries abuse IdP drift, device code flows, stale sessions, weak conditional access, helpdesk processes, SaaS integrations, and cloud role mappings. This talk presents a safe emulation framework for identity-first threat actors across AD, Entra ID, Okta-like workflows, and cloud control planes. The lab provides ATT&CK-aligned playbooks that simulate identity compromise, IdP pivoting, session abuse, and SaaS access without stealing real credentials. The focus is measurable purple-team validation: expected telemetry, detection hypotheses, failure points, and repeatable scoring.

Speakers: Samet Can Tasci, Mehmet Önder Key

SpeakerBio: Samet Can Tasci, Senior Linux Systems Engineer

Samet Can Tasci is a Senior Linux Systems Engineer and security researcher with experience across enterprise infrastructure, cloud and hybrid environments, automation, and defensive security validation.

His research interests include web defense behavior, WAF normalization gaps, parser inconsistencies, adversary-informed testing, and practical tooling for security teams.

He is the creator of WaffleX, a research prototype selected for Black Hat USA Arsenal, which focuses on semantic consistency analysis, enforcement drift, and family-level request-variant testing across modern web application defense stacks.

SpeakerBio: Mehmet Önder Key, Cyber Security Consultant

Önder Key is a cybersecurity consultant specializing in critical infrastructure security, zero-day vulnerability analysis, and offensive security. He has advised organizations in high-security sectors such as defense, aerospace, and finance, with hands-on experience in both red teaming and strategic security engineering. His work has been featured across numerous countries and platforms, contributing to the discovery of systemic vulnerabilities. Currently, he provides consultancy to TurkNet and continues to advance the global offensive security ecosystem by challenging traditional approaches to cybersecurity.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Contests - Saturday - 10:00-17:59 PDT

Title: Escalation Desk CTF

Tags: Call Center Village | Escalation Desk CTF | Contest

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 2 W218 (Call Center Village) - [Map](#)

Description:

Customer service channels are increasingly saturated with conversational text and voice AI agents. Can you convince, trick, or break enough of them to earn your shot at a live human operator in a real-world call center?

Escalation Desk is Call Center Village's capture-the-flag challenge. Start with low-pressure AI agents and learn how to spot, avoid, and exploit common pitfalls and patterns in system prompts — eventually unlocking live human operators at our partner call centers. A real-time leaderboard tracks solo and team progress, with our not-so-famous Golden Telephone Booth trophy awarded to the top participant.

Hit our minimum point threshold and earn a special Call Center Village 100 Trying black flight tag. The top individual and their team also take home the rare Call Center Village 200 OK gold flight tags. Bring your tags to Party Line, Call Center Village's after-hours telephony-themed party, and enjoy free refreshments for your spoils.

Escalation Desk is beginner (and introvert) friendly — if you can dial a phone number or use a keyboard, you can participate. Bring your own laptop and headset, or use one of our village stations. Active Noise-canceling headphones with a microphone are highly recommended.

The CTF will run during village hours, pausing when the village closes each night, and ends on Sunday at 12:00.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Contests - Sunday - 10:00-11:59 PDT

Title: Escalation Desk CTF

Tags: Call Center Village | Escalation Desk CTF | Contest

When: Sunday, Aug 9, 10:00 - 11:59 PDT

Where: LVCCW Level 2 W218 (Call Center Village) - [Map](#)

Description:

Customer service channels are increasingly saturated with conversational text and voice AI agents. Can you convince, trick, or break enough of them to earn your shot at a live human operator in a real-world call center?

Escalation Desk is Call Center Village's capture-the-flag challenge. Start with low-pressure AI agents and learn how to spot, avoid, and exploit common pitfalls and patterns in system prompts — eventually unlocking live human operators at our partner call centers. A real-time leaderboard tracks solo and team progress, with our not-so-famous Golden Telephone Booth trophy awarded to the top participant.

Hit our minimum point threshold and earn a special Call Center Village 100 Trying black flight tag. The top individual and their team also take home the rare Call Center Village 200 OK gold flight tags. Bring your tags to Party Line, Call Center Village's after-hours telephony-themed party, and enjoy free refreshments for your spoils.

Escalation Desk is beginner (and introvert) friendly — if you can dial a phone number or use a keyboard, you can participate. Bring your own laptop and headset, or use one of our village stations. Active Noise-canceling headphones with a microphone are highly recommended.

The CTF will run during village hours, pausing when the village closes each night, and ends on Sunday at 12:00.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Contests - Friday - 10:00-17:59 PDT

Title: Escalation Desk CTF

Tags: Call Center Village | Escalation Desk CTF | Contest

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 2 W218 (Call Center Village) - [Map](#)

Description:

Customer service channels are increasingly saturated with conversational text and voice AI agents. Can you convince, trick, or break enough of them to earn your shot at a live human operator in a real-world call center?

Escalation Desk is Call Center Village's capture-the-flag challenge. Start with low-pressure AI agents and learn how to spot, avoid, and exploit common pitfalls and patterns in system prompts — eventually unlocking live human operators at our partner call centers. A real-time leaderboard tracks solo and team progress, with our not-so-famous Golden Telephone Booth trophy awarded to the top participant.

Hit our minimum point threshold and earn a special Call Center Village 100 Trying black flight tag. The top individual and their team also take home the rare Call Center Village 200 OK gold flight tags. Bring your tags to Party Line, Call Center Village's after-hours telephony-themed party, and enjoy free refreshments for your spoils.

Escalation Desk is beginner (and introvert) friendly — if you can dial a phone number or use a keyboard, you can participate. Bring your own laptop and headset, or use one of our village stations. Active Noise-canceling headphones with a microphone are highly recommended.

The CTF will run during village hours, pausing when the village closes each night, and ends on Sunday at 12:00.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: ESP32 as a counter-surveillance platform

Tags: DEF CON Official Talk | Demo

When: Sunday, Aug 9, 10:00 - 10:59 PDT

Where: LVCCW Level 1 Hall 3 1006 (Main Track 1) - [Map](#)

Description:

Privacy should be accessible to all. Historically, counter-surveillance tools have been expensive, complex, and inaccessible to most individuals, often limited to well-funded researchers and costly hardware configurations. The ESP32 offers a transformative alternative. This presentation will demonstrate how an affordable microcontroller has become the foundation for a growing suite of open-source, user-friendly anti-surveillance tools. We will discuss the technical features that make the ESP32 a compelling choice for these applications, including passive 802.11 and Bluetooth monitoring, OUI-based device fingerprinting, and robust cryptographic capabilities. Applications include detecting police body cameras in operational environments, mapping Flock Safety automatic license plate recognition (ALPR) infrastructure, identifying unauthorized drones, detecting radio frequency jamming across 2.4GHz, 5GHz, and cellular bands, and tracking autonomous robots operating with known-vulnerable firmware. These tools are cost-effective and freely available. We will also consider future developments in accessible counter-surveillance hardware, such as the ESP32-S5 with 5GHz support, GPS, displays, haptics, etc. Advancing anti-surveillance culture requires designing devices that individuals are motivated to use and carry.

Speakers: Cooper "Cybertiger" Quintin, Colonel Panic, The Wrew

SpeakerBio: Cooper "Cybertiger" Quintin, Board Member at Open Archive

Cooper Quintin is a security researcher and senior public interest technologist with the EFF Threat Lab. research fellow with Citizen Lab, adviser to CoRD Research and Design, and board member of Open Archive. He has worked on projects including Rayhunter, Privacy Badger, Canary Watch, and analysis of state sponsored malware campaigns such as Dark Caracal. Cooper has given talks about security research at prestigious security conferences including Black Hat, DEFCON, Enigma Conference, and ReCon about issues ranging from IMSI Catcher detection to fem tech privacy issues to newly discovered APTs. He has also been published or quoted in publications including: The New York Times, Reuters, NPR, CNN, and Al Jazeera. Cooper has given security trainings for activists, non profit workers, and vulnerable populations around the world. He previously worked building websites for nonprofits, including Greenpeace, Adbusters, and the Chelsea Manning Support Network. Cooper was also an editor and contributor to the hacktivist journal, "Hack this Zine." In his spare time he enjoys making music, visualizing a solar-punk communitarian future, and playing with his kids.

SpeakerBio: Colonel Panic

Malware researcher by day, IoT rapid prototyper by night. Creator of Mesh-Detect and Oui-Spy. I love making things and bringing my ideas to a completed prototype rapidly. I'm Interested in privacy, digital rights, and detecting all the things.

SpeakerBio: The Wrew, Hackers.Town

Product Manager working on building pentesting platforms by day, hacker and electronics prototyper by night (and occasional weekend). Creator of VoidMantisOS for the hacker pager and SpectraMesh mesh networking protocol. Interested in security, privacy, RF, electronics and fighting digital surveillance. Listed under: just handle

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Europe's Expanding Role in Global Vulnerability Management

Tags: Policy @ DEF CON | Creator Talk/Panel

When: Saturday, Aug 8, 12:00 - 12:59 PDT

Where: LVCCW Level 2 W210-211 (Policy Village) - [Map](#)

Description:

The Common Vulnerabilities and Exposures (CVE) Program has become foundational to global cybersecurity operations. However, as vulnerability discovery accelerates and regulatory frameworks emerge, CVE is no longer just a technical reference system — it is evolving into critical infrastructure at the intersection of security and public policy. This talk presents ENISA's operational and policy role in strengthening the global CVE ecosystem, including its designation as a CVE Numbering Authority and Root CNA, its development of the EU Vulnerability Database (EUVD), and its mandate under the Cyber Resilience Act to build a Single Reporting Platform for vulnerability coordination across Europe. Moreover, the talk will explain how ENISA plans to operationalize the collected data to strengthen the overall security ecosystem. The session will explore how policy decision at EU level impact vulnerability disclosure, coordination, and data quality — and how Europe is scaling its role without fragmenting the global system. The goal is to provide a practical, but both strategic and operational perspective on how the EU's increased role in this area will ensure a more resilient and interoperable vulnerability ecosystem. (This talk will develop both talks held by ENISA at VulCon 2026)

Speakers: Nuno Rodrigues Carvalho, Razvan Gavrila

SpeakerBio: Nuno Rodrigues Carvalho, ENISA - The European Union Agency for Cybersecurity

Nuno Rodrigues Carvalho currently serves as Head of Sector of the Incident & Vulnerabilities Services within the Operations and Situational Awareness Unit (OSA) of the European Union Agency for Cybersecurity (ENISA). He leads the department in ENISA dealing with the development of Vulnerability Services (including the European Union Vulnerability Database), of the Single Reporting Platform of the Cyber Resilience Act and the Cybersecurity Incident Reporting and Analysis System (CIRAS) and the reports stemming from the NIS 2 legislation related to that system. Before joining ENISA as a Senior Threat and Vulnerability Analyst, he developed more than 15 years of experience in strategic, tactical, and operational analysis and situational awareness through roles at both national and international levels. Previously, he also worked at the European Parliament and in the banking sector.

SpeakerBio: Razvan Gavrila, ENISA - The European Union Agency for Cybersecurity

Razvan Gavrila is a seasoned cybersecurity professional with over 15 years of experience across national and EU institutions. In his current role, he oversees ENISA's work on the implementation of the EU Cyber Resilience Act and leads initiatives in product and security engineering, including the cybersecurity of AI systems. Prior to his appointment as Head of Sector for Market, Technology, and Product Security in January 2025, he served as ENISA's lead Cyber Threat Intelligence (CTI) analyst. He holds several industry-recognized certifications and a Master of Science in Computer and Information Security

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Evading EDR in ATM

Tags: Red Team Village | Misc

When: Saturday, Aug 8, 16:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 309 (Red Team Village) Tactic Table 2 - [Map](#)

Description:

ATMs in the end are a computer with windows

I will talk about EDRs and how parent-child process inheritance works

The Windows boot process, known as the boot process, is divided into several phases as we have already seen: PreBoot (initialization of BIOS/UEFI firmware and POST), Boot Manager (loading of bootmgr or bootmgfw.efi), OS Loader (execution of winload.exe to load the kernel), and Kernel Initialization (loading of ntoskrnl.exe and hal.dll, initialization of drivers and services). Finally, winlogon.exe is started to present the user interface. This process enables the transition from a powered-off state to a functional operating system through a hierarchical and verified sequence.

Regarding kernel-based EDRs (Endpoint Detection and Response), they operate in kernel mode, the most privileged level of the system (some also operate at the UEFI level), which allows them to monitor low-level activities such as system calls, memory manipulation, driver loading, and file access. By running in this mode, EDRs can detect and block advanced threats such as rootkits or persistent malware that attempt to evade user-mode protections. Their deep integration with the kernel enables real-time monitoring, behavioral analysis, and immediate response to suspicious activities during and after the boot process. EDRs are typically located in the kernel, but as mentioned, some also operate at the UEFI level. If we recall how Windows works, beneath UEFI lies SMM (System Management Mode), making this an even more complex layer to analyze and operate within.

This talk is intended for individuals interested not only in ATMs and simple cash dispensing, but in going beyond that—focusing on deeper analysis and the full experience gained when confronting these systems.

More information about the attack and the theory behind it: <https://h0km4.com/posts/DMA-Introduction/>
<https://h0km4.com/posts/telemetry-bypass/>

SpeakerBio: Arnold Jared Morales Yopez, Senior Team Lead, Grupo Salinas

Self-taught in computer security since age 12; holds a degree in Computer Forensics and Cybersecurity and is pursuing a Master's in AI and Cybersecurity.

--

Desde los 12 años, me he dedicado a la informática con un enfoque especial en la seguridad. Actualmente, a mis 22 años, sigo explorando este mundo con la misma pasión, impulsado por la constante evolución de la tecnología y su interminable curva de aprendizaje.

Cuento con una carrera en Cómputo Forense y Ciberseguridad, actualmente curso una maestría en Inteligencia Artificial y Ciberseguridad.

Certificaciones: CWEE | CAPE | CPTS | EWPTX | CRT0 | eMAPT | OSCP | OSCP+ | CEH V13 | EJPT | HTB prolabs Hades - Cybernetics - Zephyr - APTlabs | MDK



Title: Evading LLM Detection

Tags: Cryptocurrency Village | Creator Talk/Panel

When: Saturday, Aug 8, 13:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 3 1103 (Creator Stage 5) - [Map](#)

Description:

Software supply chain attacks are no longer a distant threat — they are happening at scale and extremely dangerous from a crypto exchange's POV.

As build pipelines grow more complex and dependencies multiply across npm, PyPI, SBOM, and internal registries, a single scanning layer is no longer enough to detect malicious code.

This talk focuses on an AI journey — from deploying a single AI agent to gate code merges, to architecting a full multi-agent system hardened through structured simulated exercises — along the way catching real-world attacks, including the coordinated compromise of a highly popular npm package spanning over 2 billion weekly downloads.

Speakers: Hanley Shun, Cong Zhang, ; Oscar Skjerven

SpeakerBio: Hanley Shun, OKX

Hanley has been working in information security for 10 years, with a background in penetration testing and vulnerability management. Now at OKX, channeling that offensive mindset into building secure CI/CD pipelines with AI, every day keeping customers' funds safe.

SpeakerBio: Cong Zhang, OKX

Cong has spent 5 years building SAST from the inside out — engines, rules, and the thinking behind them. From AST-level detection logic to full scanning pipelines, he knows where static analysis hits its limits. Now at OKX, he's pushing past them with AI, teaching tools to reason about supply chain risks and logic flaws that pattern matching will never catch.

SpeakerBio: ; Oscar Skjerven, OKX

No BIO available

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Every ride you take - Hacking a City's Public Transportation

Tags: AppSec Village | Creator Talk/Panel | All Audiences

When: Saturday, Aug 8, 14:10 - 14:40 PDT

Where: LVCCW Level 1 Hall 2 604 (Appsec Village) Main Stage - [Map](#)

Description:

Let's talk about some critical infrastructure that millions of people use every day: Public transportation. In this talk, I'll present some findings that I discovered in the public transportation ecosystem of one of the largest cities in Argentina, impacting more than 1.5 million people daily. Reading code, chaining vulnerabilities, weak access controls, and flawed internal designs, I got full access to core mobility systems, from buses to taxis, including DVRs, transport cards, user data, real-time tracking and administrative panels. We'll walk through the technical exploitation path, the real-world impact and the lessons learned.

SpeakerBio: Ignacio Navarro

Ignacio Navarro, an Ethical Hacker and Security Researcher from Cordoba, Argentina. With around 6 years in the cybersecurity game, he's currently working as an Application Security. Their interests include code analysis, web application security, and cloud security. Speaker at DEFCON, H2HC, Troopers, LeHACK, NorthSec, TyphoonCon, Security Fest, 8.8, among others. @Ignavarro1



[Return to Index](#) - Add to Google - ics [Calendar](#) file

The Diana Initiative - Saturday - 13:00-13:59 PDT

Title: Everything I Need to Know About Security, I Learned from Mr. Rogers

Tags: The Diana Initiative | Creator Event/Activity

When: Saturday, Aug 8, 13:00 - 13:59 PDT

Where: LVCCW Level 2 W209 (Diana Initiative) - [Map](#)

Description:

The same lessons we learned from children's programs growing up can help keep organizations safe. Kindness builds trust, and trust gets team buy-in to security processes. Diversity increases the vantage points and perspectives able to spot gaps or loopholes in technology and process. Empathy that puts us in the shoes of our users helps refine workflows, and a company that takes care of its employees reduces the likelihood of internal bad actors. Security is more about effective cooperation than a digital dogfight.

SpeakerBio: Zoe

No BIO available

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Nix Vegas Community - Friday - 15:00-15:30 PDT

Title: Everything is Nix when you squint hard enough

Tags: Nix Vegas Community | Creator Talk/Panel

When: Friday, Aug 7, 15:00 - 15:30 PDT

Where: LVCCW Level 1 Hall 4 1310 (Nix Vegas Community) - [Map](#)

Description:

How I got started with NixOS and how it's going. I'll cover my homelab migration from ubuntu & docker to NixOS & Incus w/ NixOS containers. I'll also go over how a similar process is going at my \$job, discussing packaging proprietary software into modules. I'll cover declarative hardware and software in both domains from an SRE point of view.

SpeakerBio: Jared

I'm an SRE based in \$location working for \$job.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Evidence-Based Elections and Risk-Limiting Audits

Tags: Voting Village | Creator Talk/Panel

When: Friday, Aug 7, 14:00 - 14:45 PDT

Where: LVCCW Level 2 W220 (Voting Village) (Voting Village Talks) - [Map](#)

Description:

Public trust in U.S. elections has been shaken by allegations that the 2020 presidential election was "stolen" or "rigged." While many specific claims about that election are technically incoherent or demonstrably false, it is true that the way elections are administered in the U.S.--including eligibility determinations, voting equipment, procedures, and audits--leaves room for rational doubt about whether the reported outcomes of U.S. elections are correct. Given the known vulnerabilities in voting systems, the shortcomings of election procedures in some jurisdictions, and examples of large errors in vote counts and insider malfeasance, to blithely and automatically accept reported results is naive. To deserve public trust, elections should be "evidence-based": conducted in a way that generates convincing public evidence that the reported outcome is correct. "Trust us" is not evidence. Evidence-based elections generally require demonstrably accurate eligibility determinations; recording votes primarily on hand-marked paper ballots; demonstrably secure chain of custody of voted ballots; a rigorous canvass to ensure that every validly cast ballot (and no others) was included; tabulation of the votes by hand or by machine; a compliance audit to ensure that the paper trail is trustworthy; and a properly designed, publicly confirmable audit of the reported results using the trustworthy paper trail. Conducting evidence-based elections requires avoiding the use of technology for purposes where outcome-altering malfunction or malfeasance could escape detection and correction, for instance, using electronic technology to record or transmit votes (e.g., paperless voting systems, touchscreen ballot-marking devices, cellular networks, or the Internet). Risk-limiting audits (RLAs) play an important role in evidence-based elections, providing affirmative evidence that the reported outcome is correct--or, with high probability, correcting the outcome if it is wrong. RLAs require a trustworthy paper trail. They cannot compensate for poor election administration, such as failing to keep track of voted ballots or using vulnerable technology to record or transmit votes.

SpeakerBio: Philip Stark

Philip B. Stark is Distinguished Professor of the Graduate School at the University of California, Berkeley, where he has served as department chair and associate dean. In 2007 he invented "risk-limiting audits" ("RLAs"), endorsed by the National Academies of Science, Engineering, and Medicine and the American Statistical Association, among others, and required or authorized by law in about 15 states. He designed and helped conduct the first dozen pilot RLAs, helped draft RLA legislation for several states, and has published open-source software to support RLAs. In 2012, he and David Wagner introduced "evidence-based elections," a paradigm for conducting demonstrably trustworthy elections. Stark has served on the Board of Advisors of the US Election Assistance Commission and its cybersecurity subcommittee, the Board of Directors of Verified Voting Foundation and the Election Integrity Foundation, and on the California Post Election Audit Standards Working Group. He has worked with the Secretaries of State of California, Colorado, and New Hampshire and numerous local election officials. He has testified about election integrity in state and federal courts and to legislators. He received the IEEE Cybersecurity Award for Practice, the UC Berkeley Chancellor's Award for Research in the Public Interest, and the John Gideon Award for Election Integrity. He is a fellow of the American Academy of Arts and Sciences, the American Statistical Association, and the Institute of Physics.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Evil Is Always a Bad Stylist: .NET Obfuscation with Roslyn

Tags: Red Team Village | Misc

When: Sunday, Aug 9, 10:00 - 11:59 PDT

Where: LVCCW Level 1 Hall 1 309 (Red Team Village) Tactic Table 4 - [Map](#)

Description:

Modern endpoint defenses increasingly fingerprint .NET tools not only by strings and imports, but by structure: control flow, call graphs, and overall execution “workflows.” Traditional IL obfuscation can hide obvious indicators, yet often produces highly regular flattened patterns that are easy to flag on their own.

This talk presents a Roslyn-based, source-to-source obfuscator for C# that rewrites an entire project before compilation. Using the official compiler APIs, it transforms the code’s syntax and semantic structure, reshapes control/data flow, and then recompiles the result - while keeping the program’s observable behavior intact. The output tends to look complex but “natural,” diverging both from the original tool and from the telltale patterns created by many IL-level obfuscators.

I will walk through the pipeline, show how surprisingly little code is needed to build these transformations on Roslyn, and discuss what this means for EDR, sandboxing, and ML detections that rely on graph and workflow analysis of .NET binaries.

So, anyway, on moment of submitting original Seatbelt tool (obfuscated by source) have 10/73 security vendors flagged this file as malicious (can be better)

<https://www.virustotal.com/gui/file/ec2dcecb927874d41b051633135c8a594abb40d03f6836a548b40963bf330c86/detection/f-ec2dcecb927874d41b051633135c8a594abb40d03f6836a548b40963bf330c86>

My project <https://github.com/gam4er/Loaders> differs from more well known <https://github.com/sadreck/Codeception> by implementing semantic structure obfuscation.

My point of view (sa a SOC analyst, blue teamer) on "how to hide mytool from AV" problem is: if you have a code - OBFUSCATE YOUR CODE. Stop modifying binaries

Speakers: Alexander Rodchenko, Ashley Hiram Muñoz, Eduardo Chavarro Ovalle

SpeakerBio: Alexander Rodchenko

Rodchenko Alexander is a Senior SOC Analyst at the SOC Security Research Group at Kaspersky. He began his career at OJSC Rosneft, focusing on industrial safety, troubleshooting, and audits. Currently, he investigates industry events and trends with the primary goal of integrating these insights into monitoring and threat hunting practices. Leveraging his extensive expertise, Alexander advises customers and threat detection/hunting teams on the optimal response to emerging threats and trends. In addition to speaking at Positive Hack Days (twice) and BSides Zurich 2023, he has also been a speaker at CodeBlue 2024 and BlackHat MEA 2024.

SpeakerBio: Ashley Hiram Muñoz, Kaspersky - Incident Response Specialist

I currently work as an Incident Response Specialist on Kaspersky's Global Emergency Response Team (GERT). I live in Mexico and have over seven years of experience in Incident Response, Digital Forensics, Malware Analysis, and Reverse Engineering. Before joining DFIR, I worked for two years as a Penetration Tester.

I have collaborated on various Threat Hunting and Threat Intelligence projects.

Additionally, I have been a speaker at international events such as DEFCON (La Villa Hacker), BSides, Ekoparty, 8.8, HackGDL, BugCON, Pwnterrey, and others. I currently teach the Digital Forensics, Malware Analysis, and Incident Response

modules in an information security diploma program at UNAM (Universidad Nacional Autónoma de México).

Certifications: GREM, GCFA, GCFR, eCTHP, CHFI.

--

Actualmente me desempeño como Incident Response Specialist en el Global Emergency Response Team (GERT) de Kaspersky, cuento con +6 años de experiencia realizando Respuesta a Incidentes, Análisis Forense Digital, Análisis de Malware y Reversing; previo a dedicarme a DFIR laboré 2 años como Penetration Tester.

He colaborado en distintos proyectos de Threat Hunting y Threat Intelligence.

Adicionalmente, he sido ponente en eventos internacionales como DEFCON (La Villa Hacker), BSides, Ekoparty, 8.8, BugCON, etc.

Actualmente soy profesor de los módulos de Análisis Forense, Análisis de Malware y Respuesta a Incidentes en un diplomado de seguridad de la información de la UNAM.

Certificaciones: GREM, GCFA, eCTHP, CHFI.

SpeakerBio: Eduardo Chavarro Ovalle, DFIR Group Manager at Kaspersky - GERT

Eduardo Chavarro Ovalle, DFIR Group Manager for Americas, member of Kaspersky GERT Team. Student of DBA in ML and AI and MSc in Cybersecurity with more than 20 years of experience in cybersecurity, DFIR, eDiscovery, and threat analysis. GCIH | GRID | GCFA | CISM | CHFI | CPTE | SFCP | ITIL.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: EvilEssid: Evading Wireless Intrusion Prevention Systems

Tags: Red Team Village | Misc

When: Friday, Aug 7, 16:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 309 (Red Team Village) Tactic Table 1 - [Map](#)

Description:

What if a rogue access point could evade a Wireless Intrusion Prevention System (WIPS) while operating in plain sight?

In this hands-on tactic, participants will learn how EvilEssid, a wireless evasion technique, exploits weaknesses in how WIPS solutions identify, classify, and trust wireless networks. Rather than focusing solely on theory, attendees will actively build, configure, and operate EvilEssid in a controlled lab environment. Through a series of guided exercises, participants will gain practical experience deploying rogue access points, understanding WIPS detection logic, and applying wireless identity manipulation techniques to evade common defensive controls. The workshop will demonstrate how attackers can establish malicious wireless infrastructure that remains undetected while creating opportunities for credential harvesting, traffic interception, and adversary-in-the-middle operations. Attendees will use the EvilEssid tool to reproduce the attack chain step-by-step. Each exercise is designed to provide hands-on exposure to offensive wireless tradecraft while encouraging participants to experiment. Beyond the offensive techniques, the workshop will also explore defensive implications, helping participants understand the limitations of current WIPS technologies and identify practical approaches to improve wireless threat detection. By the end of the session, attendees will have deployed a rouge access point using EvilEssid themselves, validated successful WIPS evasion in a lab environment, and gained a deeper understanding of both the offensive and defensive aspects of advanced wireless operations.

Fundamentals • ESSID

• BSSID

• Deauthentication attacks • Evil Twin attack Understanding WIPS and Its Detection Models • What is a WIPS • How it works and detection techniques • Evil Twin attack vs WIPS Identifying the Weakness Advancing the Evil Twin Technique • Human targets • Crafting a WIPS-evasive Evil Twin EvilEssid tool: Design and Implementation • Overview • Key concepts behind the tool • Features and usage Conclusions and Countermeasures

SpeakerBio: Miguel Fernandez

Colombian cybersecurity researcher based in China with over 15 years of experience in offensive security, penetration testing, and applied security research.

His work focuses on developing and validating novel attack and defense techniques, challenging existing security assumptions across areas such as wireless security, social engineering, and real-world adversarial methodologies.

He has presented at international conferences including Codegate, Overdrive, CIS, Xcon x Hacking group ,WAIC, Hackprove world, Tencent security saloon and multiple PRC cyber security meetups.

His research is grounded in the scientific method, emphasizing experimentation, reproducibility, and practical validation.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Execution of modern techniques to start/improve your career in Incident Response

Tags: La Villa Community | Creator Workshop

When: Saturday, Aug 8, 14:00 - 15:59 PDT

Where: LVCCW Level 1 Hall 4 1416 (La Villa Community) Workshops/Chillout - [Map](#)

Description:

Practicaremos algunas técnicas modernas que utilizamos en equipos globales de Respuesta a Incidentes para procesar y analizar evidencias digitales durante ataques cibernéticos, y responder con conclusiones acertadas en un lapso muy corto.

Este taller está dirigido para quienes desconocen cómo empezar su carrera en DFIR o buscan afinar sus técnicas de investigación.

Habrà un pequeño CTF de un incidente de Ransomware con regalos para los ganadores.

SpeakerBio: Ashley Hiram Muñoz, Kaspersky - Incident Response Specialist

I currently work as an Incident Response Specialist on Kaspersky's Global Emergency Response Team (GERT). I live in Mexico and have over seven years of experience in Incident Response, Digital Forensics, Malware Analysis, and Reverse Engineering. Before joining DFIR, I worked for two years as a Penetration Tester.

I have collaborated on various Threat Hunting and Threat Intelligence projects.

Additionally, I have been a speaker at international events such as DEFCON (La Villa Hacker), BSides, Ekoparty, 8.8, HackGDL, BugCON, Pwnterrey, and others. I currently teach the Digital Forensics, Malware Analysis, and Incident Response modules in an information security diploma program at UNAM (Universidad Nacional Autónoma de México).

Certifications: GREM, GCFA, GCFR, eCTHP, CHFI.

--

Actualmente me desempeño como Incident Response Specialist en el Global Emergency Response Team (GERT) de Kaspersky, cuento con +6 años de experiencia realizando Respuesta a Incidentes, Análisis Forense Digital, Análisis de Malware y Reversing; previo a dedicarme a DFIR laboré 2 años como Penetration Tester.

He colaborado en distintos proyectos de Threat Hunting y Threat Intelligence.

Adicionalmente, he sido ponente en eventos internacionales como DEFCON (La Villa Hacker), BSides, Ekoparty, 8.8, BugCON, etc.

Actualmente soy profesor de los módulos de Análisis Forense, Análisis de Malware y Respuesta a Incidentes en un diplomado de seguridad de la información de la UNAM.

Certificaciones: GREM, GCFA, eCTHP, CHFI.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Exfil Everything: A Year of Stealing Data from AI Agents

Tags: Bug Bounty Village | Creator Talk/Panel

When: Saturday, Aug 8, 14:00 - 14:30 PDT

Where: LVCCW Level 2 W206-207 (Bug Bounty Village) - [Map](#)

Description:

For two decades, XSS was the king of data theft — exploiting trust boundaries in a victim's browser to exfiltrate sensitive data and perform malicious actions. AI-powered interfaces have introduced new ways to deliver XSS to victims alongside an entirely new bug class that has emerged as the most impactful vulnerability pattern in modern AI applications. The parallels between XSS and AI data exfiltration are striking — both exploit trust boundaries to force a system into performing unintended actions on behalf of a victim but the attack surface in AI is broader, spanning web interfaces, mobile apps, wearables, and any client consuming agent output. The exfiltration channels are diverse: markdown image rendering, iframe and HTML tag injection, sandbox escapes, native platform connectors, network connectivity tools, javascript: URI schemes, link unfurling side channels, MCP server poisoning, and multi-step agent tool-abuse chains. In this talk, two bug hunters who've spent the past year exploiting these vulnerabilities across production applications break it down and walk through real attack chains, demonstrate how we bypass common mitigations and share the bypass techniques we've developed. We'll cover how to threat model AI applications, identify viable attack paths, and select delivery mechanisms to weaponize end-to-end exploits. Beyond offense, we'll discuss the mitigations we've encountered, what actually works, what doesn't, and emerging trends in agentic AI and autonomous tool use mean for the next wave of vulnerabilities hunters should be watching for. Leave with: (1) a clear mental model of AI data exfiltration as a bug class and how it relates to familiar web primitives, (2) concrete attack techniques and bypass methods, (3) practical threat modeling for identifying exfil paths in AI agents and applications, and (4) visibility into upcoming trends and bug classes they should be hunting as AI systems gain more autonomy and connectivity.

Speakers: Ads Dawson, Mike "TakSec" Takahashi

SpeakerBio: Ads Dawson, Staff AI Security Researcher, OWASP GenAI Security Project founder

Ads Dawson founded the OWASP GenAI Security Project and led it to flagship status — the fastest in OWASP history. As a Staff AI Security Researcher at Dreadnode, he specializes in exploiting ML and AI systems, harnessing AI for offensive cybersecurity through capability development and exploit development, and conducting red team operations against frontier models for government, military, and tier-1 labs. He is lead author of AIRTbench (arXiv), the first benchmark for autonomous AI red teaming in LLMs, and author of AI Native LLM Security (Packt, 2025).

A senior red team operator with BT6 (the frontier AI red team), ranked #2 in Canada on HackerOne (2025/2026), and selected for Meta's MBBRC live hacking event, Ads is a HackerOne US South Ambassador, BugCrowd Hacker Advisory Board member, MITRE AI Working Group contributor, and leads the OWASP Toronto chapter. He spoke at Bug Bounty Village DC33 on the BT6 AI jailbreaking panel and is also presenting "Exfil Everything: A Year of Stealing Data from AI Agents" at Bug Bounty Village DC34 (schedule pending publication).

SpeakerBio: Mike "TakSec" Takahashi, AI Red Team Researcher, Zenity

Mike Takahashi, aka TakSec, is an AI Red Team Researcher at Zenity; member of BT6; and Bug Bounty Hunter focused on breaking AI systems. He has submitted 400+ vulnerabilities across major bug bounty programs and top ranking on both Anthropic's Safety Bug Bounty Program on HackerOne and Mozilla's Odin GenAI Bug Bounty Program. His work targets prompt injection, data exfiltration, and AI agent security.



Title: Exploit Bluetooth Low Energy with BLESPlloit and optional ESP32

Tags: Embedded Systems Village | Creator Event/Activity

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 2 503 (Embedded Systems Village) - [Map](#)

Description:

Discover how easy it is to fingerprint and control nearby BLE devices with a tap on your phone - yes, including iPhone that gets BLE superpowers with with an external ESP32. Scan remotely, clone and simulate BLE devices, test a popular headset for known vulnerabilities (or perhaps uncover a new one?) and take control of a robotic dog. Already know some BLE? Crack open our smart safe and claim the BLESPlloit hardware reward inside!

SpeakerBio: Slawomir Jasek, BLESPlloit.it

Seasoned trainer, speaker and IT security consultant with over two decades of expertise. Developed secure embedded systems certified to use by national agencies, participated in dozens assessments of systems, applications, firmware and hardware security for leading financial companies, largest manufacturers and innovative startups. Currently focuses on security research of new technologies (especially Bluetooth Low Energy and NFC/RFID) and provides training in regards to security of devices - based among others on contemporary electronic access control systems and smart locks. Beyond consulting on secure design for various software and hardware projects, impulsively acquires more and more BLE and NFC devices and enjoys reversing and breaking them. Loves sharing his knowledge via trainings, workshops, talks and open source hackme's (<https://www.smartlockpicking.com/>) – at OrangeCon, BlackHat, HackInTheBox, Hardwear.io, HackInParis, Deepsec, Appsec EU, BruCon, Confidence, and many others, including private on-demand sessions.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Exploit Bluetooth Low Energy with BLESPlloit and optional ESP32

Tags: Embedded Systems Village | Creator Event/Activity

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 2 503 (Embedded Systems Village) - [Map](#)

Description:

Discover how easy it is to fingerprint and control nearby BLE devices with a tap on your phone - yes, including iPhone that gets BLE superpowers with with an external ESP32. Scan remotely, clone and simulate BLE devices, test a popular headset for known vulnerabilities (or perhaps uncover a new one?) and take control of a robotic dog. Already know some BLE? Crack open our smart safe and claim the BLESPlloit hardware reward inside!

SpeakerBio: Slawomir Jasek, BLESPlloit.it

Seasoned trainer, speaker and IT security consultant with over two decades of expertise. Developed secure embedded systems certified to use by national agencies, participated in dozens assessments of systems, applications, firmware and hardware security for leading financial companies, largest manufacturers and innovative startups. Currently focuses on security research of new technologies (especially Bluetooth Low Energy and NFC/RFID) and provides training in regards to security of devices - based among others on contemporary electronic access control systems and smart locks. Beyond consulting on secure design for various software and hardware projects, impulsively acquires more and more BLE and NFC devices and enjoys reversing and breaking them. Loves sharing his knowledge via trainings, workshops, talks and open source hackme's (<https://www.smartlockpicking.com/>) – at OrangeCon, BlackHat, HackInTheBox, Hardwear.io, HackInParis, Deepsec, Appsec EU, BruCon, Confidence, and many others, including private on-demand sessions.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Exploit Bluetooth Low Energy with BLESPlloit and optional ESP32

Tags: Embedded Systems Village | Creator Event/Activity

When: Sunday, Aug 9, 10:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 2 503 (Embedded Systems Village) - [Map](#)

Description:

Discover how easy it is to fingerprint and control nearby BLE devices with a tap on your phone - yes, including iPhone that gets BLE superpowers with with an external ESP32. Scan remotely, clone and simulate BLE devices, test a popular headset for known vulnerabilities (or perhaps uncover a new one?) and take control of a robotic dog. Already know some BLE? Crack open our smart safe and claim the BLESPlloit hardware reward inside!

SpeakerBio: Slawomir Jasek, BLESPlloit.it

Seasoned trainer, speaker and IT security consultant with over two decades of expertise. Developed secure embedded systems certified to use by national agencies, participated in dozens assessments of systems, applications, firmware and hardware security for leading financial companies, largest manufacturers and innovative startups. Currently focuses on security research of new technologies (especially Bluetooth Low Energy and NFC/RFID) and provides training in regards to security of devices - based among others on contemporary electronic access control systems and smart locks. Beyond consulting on secure design for various software and hardware projects, impulsively acquires more and more BLE and NFC devices and enjoys reversing and breaking them. Loves sharing his knowledge via trainings, workshops, talks and open source hackme's (<https://www.smartlockpicking.com/>) – at OrangeCon, BlackHat, HackInTheBox, Hardware.io, HackInParis, Deepsec, Appsec EU, BruCon, Confidence, and many others, including private on-demand sessions.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Social Gatherings/Events - Friday - 18:00-19:59 PDT

Title: Exploit Your Own Story

Tags: Meetup | Memorial Chamber

When: Friday, Aug 7, 18:00 - 19:59 PDT

Where: LVCCW Level 3 W302 (Memorial Chamber) - [Map](#)

Description:

You've spent the con finding the thread that unravels a system. Come find the one in you.

I've spent 27 years planning DEF CON's logistics — audio, stages, coffee, all of it. Three years ago I started writing for the first time in decades, and it turned into something I never expected: work published in magazines, a book underway, and a doorway into what I can only call a mystical experience — the kind where the page starts telling you things you didn't know you knew.

Women's voices are at the center of this — we carry stories that go unheard far too often, and this is a room built to change that. And there are conscious men in this community whose words matter too, and who are welcome here.

This is an open space to talk about the path — publishing, books, or just the story you've never told anyone. Bring a story, bring a question, or just come listen.

No credentials required.

SpeakerBio: Charel "1C0nur3r" Morris

No BIO available

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Social Gatherings/Events - Thursday - 18:00-19:59 PDT

Title: Exploit Your Own Story

Tags: Meetup | Memorial Chamber

When: Thursday, Aug 6, 18:00 - 19:59 PDT

Where: LVCCW Level 3 W302 (Memorial Chamber) - [Map](#)

Description:

You've spent the con finding the thread that unravels a system. Come find the one in you.

I've spent 27 years planning DEF CON's logistics — audio, stages, coffee, all of it. Three years ago I started writing for the first time in decades, and it turned into something I never expected: work published in magazines, a book underway, and a doorway into what I can only call a mystical experience — the kind where the page starts telling you things you didn't know you knew.

Women's voices are at the center of this — we carry stories that go unheard far too often, and this is a room built to change that. And there are conscious men in this community whose words matter too, and who are welcome here.

This is an open space to talk about the path — publishing, books, or just the story you've never told anyone. Bring a story, bring a question, or just come listen.

No credentials required.

SpeakerBio: Charel "1C0nur3r" Morris

No BIO available

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Exploiting Private 5G: Unauthenticated Access to Databases and Control Plane DoS via Fuzzing

Tags: Red Team Village | Misc

When: Friday, Aug 7, 11:00 - 11:59 PDT

Where: LVCCW Level 1 Hall 1 309 (Red Team Village) Workshop Tactic Table 5 - [Map](#)

Description:

Abstract—This presents an exhaustive empirical security analysis of a real-world private 5G network deployment, serving as a direct and explicit extension of our preceding research, "Security Analysis of a Real-World Private 5G Network Deployment through Pen Testing and Fuzzing." While our initial study successfully identified control-plane weaknesses and performance degradation via protocol mutation, this continuation focuses on four critical, highly exploitable attack vectors. Specifically, we detail three severe data-layer attacks stemming from the unauthenticated internal network exposure of MongoDB (Port 27017), Elasticsearch (Port 9200), and Kibana (Port 5601). These exposures permitted the complete, unauthorized extraction of the network's most sensitive cryptographic assets (including Permanent Keys and active session keys) and granted adversaries unauthorized manipulation of the security monitoring apparatus. Additionally, we introduce a newly discovered, critical Denial of Service (DoS) attack targeting the Access and Mobility Management Function (AMF) signaling interface on Port 11000, which leverages protocol fuzzing to induce memory corruption and permanently halt User Equipment (UE) registration. By synthesizing these empirical findings, this report provides a multi-layered analysis of the cascading failures that emerge when enterprise IT vulnerabilities intersect with mission-critical 5G telecommunications infrastructure.

SpeakerBio: Aumkareshwar DS

I am a Computer Science graduate student at California State Polytechnic University, Pomona, passionate about cybersecurity, network security, and ethical hacking. Currently, I work as a Research Assistant at PolySec Lab, where I focus on 5G network security, including authentication, subscriber identity protection, and threat mitigation. My research helps enhance mobile security and protect data from cyber threats.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Blacks In Cyber Village - Saturday - 14:00-14:55 PDT

Title: Exploring Security Features in the Armv8-M Architecture

Tags: Blacks In Cyber Village | Creator Talk/Panel

When: Saturday, Aug 8, 14:00 - 14:55 PDT

Where: LVCCW Level 3 W322-W324 (BIC Village) - [Map](#)

Description:

Join us for an in-depth session exploring the critical security features embedded within the Armv8-M architecture. We'll dive into TrustZone for Cortex-M, the PACBTI Extension, and the Debug Authentication/Unprivileged Debug Extension, providing clear explanations of their functionalities and the motivations behind their development. Discover how these advanced features contribute to robust embedded system security.

Speakers: Ian Harris, Jacob Gutierrez

SpeakerBio: Ian Harris, University of California, Irvine

Ian Harris is a Professor at the University of California, Irvine, specializing in computer science with a strong focus on embedded systems and security. They bring a rich background in hardware design verification and security, and their research encompasses secure hardware/software systems. Ian also teaches courses related to embedded systems and has presented at cybersecurity conferences.

SpeakerBio: Jacob Gutierrez, Cybersecurity Professional / Community Speaker

Jacob Gutierrez is a recent Computer Science graduate with a keen interest in embedded systems and their security. They are passionate about contributing to the cybersecurity community and sharing their knowledge.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

IoT Village - Saturday - 10:00-17:59 PDT

Title: Expose Hidden Surveillance in Everyday Tech

Tags: IoT Village | Creator Event/Activity

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 215 (IoT Village) - [Map](#)

Description:

Join the Ludlow Institute Surveillance Mission. Dump firmware, capture packets, probe APIs, or tear devices apart however you like. Prizes up for grabs.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

IoT Village - Friday - 10:00-17:59 PDT

Title: Expose Hidden Surveillance in Everyday Tech

Tags: IoT Village | Creator Event/Activity

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 215 (IoT Village) - [Map](#)

Description:

Join the Ludlow Institute Surveillance Mission. Dump firmware, capture packets, probe APIs, or tear devices apart however you like. Prizes up for grabs.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

IoT Village - Sunday - 10:00-13:59 PDT

Title: Expose Hidden Surveillance in Everyday Tech

Tags: IoT Village | Creator Event/Activity

When: Sunday, Aug 9, 10:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 1 215 (IoT Village) - [Map](#)

Description:

Join the Ludlow Institute Surveillance Mission. Dump firmware, capture packets, probe APIs, or tear devices apart however you like. Prizes up for grabs.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Exposed Data Centers: Bypass IT Security, Crank Up the Heat

Tags: ICS Village | Creator Talk/Panel

When: Friday, Aug 7, 17:30 - 17:59 PDT

Where: LVCCW Level 1 Hall 3 801 (Creator Stage 1) - [Map](#)

Description:

As data center numbers are increasing in the US and around the world, they are becoming a source of tension politically, environmentally, and economically, and are becoming high-value critical infrastructure. The threats to these data centers will rise soon as activists, cybercriminals, and nation-states target them. Unlike what has been seen recently with kinetic attacks on data centers in conflict zones, cyberattacks have a larger range and can affect a wider population.

We wanted to explore unconventional threats against data centers. Using open-source intelligence and our patented (US12267344B1) geostalking techniques, we were able to map out data centers in the United States and overlay that with the exposed infrastructure that would directly be used in the operation of the data center itself. This includes building automation and energy supply as examples.

Afterwards, we were left with the locations of 1,063 data centers that had 6,300 high-confidence industrial control systems exposed to the internet. This information went through a five-layer filtering process to result in these high-confidence exposed systems, based on the banner responses received from these devices. Of these 6,300 devices, 964 devices (15.3%) have a CVSS score of 9.0 or above, and 88.7% of the entire dataset is inherently vulnerable due to the use of protocols that were never designed to be exposed to the internet.

Armed with this information, an attacker could circumvent even the best IT security with exposed systems that might directly or indirectly affect data center operations. In today's geopolitical climate, exposed systems in near proximity to data centers are at higher risk of cyberattacks. Due to diverse applications across personal, corporate, or even government use, the repercussions of a data center outage will have effects far wider than just the data center itself.

Speakers: Stephen Hilt, Numaan Huq

SpeakerBio: Stephen Hilt

Stephen J. Hilt is a seasoned threat researcher specializing in industrial control systems (ICS) security, cybercrime investigations, and advanced persistent threats. With extensive experience in uncovering complex attacks targeting critical infrastructure, he has contributed to numerous high-impact reports and global threat intelligence initiatives. Stephen's work bridges deep technical expertise with strategic analysis, enabling organizations to better understand and defend against emerging cyber threats. His research has been presented at leading security conferences and published in widely respected industry reports, reflecting his commitment to advancing the security of interconnected systems worldwide.

SpeakerBio: Numaan Huq

No BIO available

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Extending Shared Threat Models with the Application Attack Matrix

Tags: AppSec Village | Creator Talk/Panel | All Audiences

When: Sunday, Aug 9, 11:10 - 11:40 PDT

Where: LVCCW Level 1 Hall 2 604 (Appsec Village) Main Stage - [Map](#)

Description:

Shared threat frameworks have enabled consistent communication and coordination across vulnerability researchers, PSIRTs, vendors, and defenders. However, as attackers increasingly operate at the application layer (abusing software supply chains, runtime behavior, and trusted cloud workflows) defenders face challenges applying existing models consistently. This session presents lessons from the Application Attack Matrix, a community-driven research effort involving contributors from Mandiant (Google Cloud), Microsoft, AWS, Meta, Oligo Security, and others, and uses the ByBit / Safe{Wallet} incident to illustrate why application-layer technique modeling is increasingly important.

SpeakerBio: J Fridley

J. Fridley is a Senior Solutions Engineer at Oligo Security, helping teams secure modern cloud environments with deep runtime visibility. He previously led and supported Solutions Engineering teams at Snyk and has a background as a software engineer and technical project lead. J also brings nearly two decades of military service with the U.S. Navy and Army National Guard.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Extension Hollowing: Abusing Chrome's Extension Trust Model

Tags: Red Team Village | Misc

When: Friday, Aug 7, 14:00 - 14:59 PDT

Where: LVCCW Level 1 Hall 1 309 (Red Team Village) Workshop Stage 2 - [Map](#)

Description:

Chrome controls over 65% of worldwide browser usage, with 100,000+ extensions on the Chrome Web Store. Enterprises rely on Chrome's built-in policies, such as extension allowlisting, WebStore integrity checks, and forced installed extensions to keep their endpoints clean. Those controls are broken. Extension Hollowing is a new technique that completely bypasses Chrome's integrity verification of WebStore extensions. By hollowing out a legitimate allowlisted extension and replacing or backdooring its internals, an attacker can silently deploy extension arbitrary code inside the browser, defeating allowlisting, bypassing signature checks, and inheriting the full permission set of the original extension (and extending it if desired). This talk will show how hollowed extensions can function as a fully capable C2 via a new Chrome extension mythic agent which will be released after this talk called Hades. Attendees will get to sit down and play with this c2 framework as well as embedding it into trusted extensions via extension hollowing. We will then walk through the specific Chrome enterprise policies designed to prevent this, and how to bypass them. The technique extends beyond Chrome to other Chromium-based browsers including Edge. TLDR; This talk will demonstrate live exploitation, discuss what EDRs are (and aren't) keying on, cover which mitigation strategies actually work, and why most deployed configurations don't. In addition attendees will get to sit down and actually embed a custom Chrome extension mythic agent inside of trusted extensions, bypassing active policies and showing how to dynamically load and run code in the latest versions of Chrome.

SpeakerBio: Gordon Long

Gordon Long is the President and CEO of LegioX Cyber Technologies and is a Senior Offensive Security Engineer at Zoom. He also teaches as an Adjunct Professor at George Mason University in the Digital Forensics Master's Program. His favorite areas of cybersecurity include EDR evasion and cyber deception. His X handle is @ethicalhax and github is under AsaurusRex.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

OSINT For Good Community - Friday - 10:00-17:59 PDT

Title: F1NDX OSINT Educational Series

Tags: OSINT For Good Community | Creator Event/Activity

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 4 1307 (OSINT4Good Community) - [Map](#)

Description:

The OSINT Educational Series is a 3-level series that introduces Open-Source Intelligence (OSINT). It covers data collection, social media analysis, and investigative techniques, showing how publicly available information is used in cybersecurity and intelligence. Volunteers will be on hand to help you get started and answer questions if you get stuck! Complete all 3 levels and earn a digital badge!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

OSINT For Good Community - Sunday - 10:00-13:59 PDT

Title: F1NDX OSINT Educational Series

Tags: OSINT For Good Community | Creator Event/Activity

When: Sunday, Aug 9, 10:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 4 1307 (OSINT4Good Community) - [Map](#)

Description:

The OSINT Educational Series is a 3-level series that introduces Open-Source Intelligence (OSINT). It covers data collection, social media analysis, and investigative techniques, showing how publicly available information is used in cybersecurity and intelligence. Volunteers will be on hand to help you get started and answer questions if you get stuck! Complete all 3 levels and earn a digital badge!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

OSINT For Good Community - Saturday - 10:00-17:59 PDT

Title: F1NDX OSINT Educational Series

Tags: OSINT For Good Community | Creator Event/Activity

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 4 1307 (OSINT4Good Community) - [Map](#)

Description:

The OSINT Educational Series is a 3-level series that introduces Open-Source Intelligence (OSINT). It covers data collection, social media analysis, and investigative techniques, showing how publicly available information is used in cybersecurity and intelligence. Volunteers will be on hand to help you get started and answer questions if you get stuck! Complete all 3 levels and earn a digital badge!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Factory Floor MVP Incident Response Challenge

Tags: AppSec Village | Creator Event/Activity || All Audiences

When: Saturday, Aug 8, 13:00 - 14:59 PDT

Where: LVCCW Level 1 Hall 2 604 (Appsec Village) POD 4 - [Map](#)

Description:

Defend the Factory. Beat the Attack. The Factory Floor MVP Incident Response Challenge is a fast-paced, interactive card-and-dice game where teams investigate cyberattacks against a modern manufacturing environment. Use strategy, collaboration, and a little luck to uncover attacker activity before production or safety is impacted. Players will walk away with practical insights into OT security, firmware and SBOM analysis, incident response, and the challenges of protecting connected industrial systems.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Factory Floor MVP Incident Response Challenge

Tags: AppSec Village | Creator Event/Activity || All Audiences

When: Friday, Aug 7, 13:00 - 14:59 PDT

Where: LVCCW Level 1 Hall 2 604 (Appsec Village) POD 3 - [Map](#)

Description:

Defend the Factory. Beat the Attack. The Factory Floor MVP Incident Response Challenge is a fast-paced, interactive card-and-dice game where teams investigate cyberattacks against a modern manufacturing environment. Use strategy, collaboration, and a little luck to uncover attacker activity before production or safety is impacted. Players will walk away with practical insights into OT security, firmware and SBOM analysis, incident response, and the challenges of protecting connected industrial systems.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Red Team Village - Friday - 10:00-11:59 PDT

Title: Falco Hunt: Evading Runtime Detection in Kubernetes

Tags: Red Team Village | Misc

When: Friday, Aug 7, 10:00 - 11:59 PDT

Where: LVCCW Level 1 Hall 1 309 (Red Team Village) Tactic Table 4 - [Map](#)

Description:

Falco is one of the most widely deployed cloud-native runtime security tools, relied upon to detect suspicious behavior across containers and Kubernetes environments. But what happens when attackers understand the rules better than defenders? In this hands-on tactic, attendees will compromise a Kubernetes environment while interacting directly with Falco detections in real time. Participants will execute common attacker actions including secret harvesting, privilege escalation attempts, reverse shell execution, and lateral movement, then iteratively adapt their tradecraft to evade or blend around runtime detections. Along the way, attendees will learn how Falco rules work, where syscall-based detection succeeds, where it struggles, and how attackers abuse assumptions in default rule sets. The session emphasizes practical detection engineering lessons for both offensive and defensive practitioners.

SpeakerBio: Michael Reimsbach, Product Security Specialist at SAP

Michael is a Product Security Specialist at SAP, working with the SAP Cloud Infrastructure security team. His focus areas include vulnerability management, secrets management, and building secure internal services.

He obtained multiple industry certifications such as OSCP, GCPN, and CISSP.

A healthy dose of paranoia led him to explore OSINT and the surprising power of publicly available information.

Beyond his day-to-day work, Michael is an active member of the cybersecurity community and helps organize BSides Luxembourg.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Farsight: Turning OSINT into Actionable Attack Surface Intelligence

Tags: Intro/Beginner | AppSec Village | Creator Event/Activity

When: Friday, Aug 7, 14:00 - 14:59 PDT

Where: LVCCW Level 1 Hall 2 604 (Appsec Village) Arsenal - [Map](#)

Description:

Farsight is an open-source reconnaissance and threat intelligence framework designed to transform fragmented OSINT workflows into a unified, automated intelligence pipeline. Traditional reconnaissance relies on multiple disconnected tools, manual correlation, and inconsistent outputs, limiting scalability and efficiency.

Speakers: Arif, Sai Vernekar, Seedon D'Souza, kvprashant

SpeakerBio: Arif

Senior Security Engineer with 5+ years of experience helping companies build and ship secure products without slowing down innovation. I specialize in Web, API, and Mobile Pentesting, Cloud Security, Threat Modeling, and embedding scalable SSDLC practices. My security journey began with curiosity and evolved into real-world impact—during an audit, I uncovered a critical flaw that could've exposed sensitive internal data. At Poshmark, I've led third-party library risk assessments, performed architecture reviews for key features, and rolled out secure coding practices across engineering. My threat modeling work improved early risk detection by 40%. Outside of work, I run hands-on security workshops, organize CTFs, and speak at conferences like c0c0n and Seaside. I'm open to the chance to solve real-world security challenges. Let's connect and build secure systems that scale.

SpeakerBio: Sai Vernekar

Sai Santosh Vernekar is a seasoned Application Security Practitioner with over a decade of expertise in application security. Over his career, Sai has undertaken secure code review, DAST, Devsecops, penetration testing as well as threat modeling. He currently works as Senior Security Engineer at Kohl's. His keen interest lies in Cloud Security & secure CI/CD implementations.

SpeakerBio: Seedon D'Souza

Hardware security expert with 10+ years in RF hacking, drone security, and exploitation. Speaker at Seaside Goa. Formerly at Sony, now at Festo.

SpeakerBio: kvprashant

Prashant Venkatesh is an information security expert with over 20 years of experience. He presently works as, Product security Leader

Prashant is an enthusiastic participant in the field who consistently coordinates, reviews papers, and presents his work at numerous InfoSec conferences, including at Nullcon and c0c0n. He is also active through the OWASP Bay Area chapter Leadership and he is co-founder of annual Seaside Conference.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Feet Feud (Hacker Family Feud)

Tags: Feet Feud (Hacker Family Feud) | Contest

When: Saturday, Aug 8, 22:00 - 23:59 PDT

Where: LVCCW Level 1 Hall 1 100 (Contest Stage) - [Map](#)

Description:

Feet Feud (Hacker Family Feud) is a Cybersecurity-themed Family Feud style game arranged by members of the OnlyFeet CTF team and hosted by Toeb3rius (aka Tib3rius). Both survey questions and their answers are crowd-sourced from the Cybersecurity community. Two teams (Left Foot and Right Foot) captained by Ali Diamond and John Hammond and comprised of audience members go head to head, trying to figure out the top answers to the survey questions.

Attendees can either watch the game or volunteer to play on one of the two teams. Audience participation is also encouraged if either of the two teams fails to get every answer of a survey question.

Ultimately Feet Feud is about having a laugh, watching people in the industry attempt to figure out what randomly surveyed people from the Cybersecurity community put as answers to a number of security / tech related questions.

Participant Prerequisites

Participants are chosen by team captains from the audience at the start of the show. In order to be fair, we try to select participants from all seating areas, so folks who show up later than others still have a chance to volunteer.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Field Notes on Offensive Agents: Reusability, Reliability, and What Breaks

Tags: Adversary Village | Creator Talk/Panel

When: Saturday, Aug 8, 13:30 - 13:59 PDT

Where: LVCCW Level 1 Hall 3 1105 (Creator Stage 3) - [Map](#)

Description:

Offensive agents are easy to demo, but much harder to make useful across real adversary emulation work. Key challenges lie in making agents reusable and reliable across different assessment types, tech stacks and doing so, as models, tools, and environments change.

This talk shares lessons from designing, deploying, and refining a suite of modular offensive agents used in real client engagements. We will cover what made the agents reusable, where they broke against real-world complexity, and how we evaluated their effectiveness over time as prompts degraded, models drifted, and underlying tools evolved. The session is framework-agnostic and vendor-neutral.

Attendees will leave with a practical model for building composable offensive agents that remain useful and reliable across attack types.

Speakers: Dominika Pietrzak, Ibai Castells

SpeakerBio: Dominika Pietrzak, Offensive AI Engineer

Building AI-led tooling to scale offensive security operations.

SpeakerBio: Ibai Castells, Senior Red Team Hive Member

Senior Red Teamer and Red Team Capability Lead at CovertSwarm. Passionate about Windows, AD, malware dev and offensive tool engineering. Currently exploring how AI can be integrated in Red Team workflows. I drop my latest research, malware dev, and how-tos on my blog and GitHub.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Filibuffer Overflow: Hackers Stage A Congressional Hearing

Tags: Policy @ DEF CON | Creator Interactive Talk/Panel

When: Friday, Aug 7, 16:30 - 17:59 PDT

Where: LVCCW Level 2 W210-211 (Policy Village) - [Map](#)

Description:

Speakers: Katherine Pratt, Jeff Rothblum, Maurice Turner, Ayan Islam, Beau Woods

SpeakerBio: Katherine Pratt, Microsoft

Katherine Pratt is a senior security engineer and operator on the AI Red Team at Microsoft. She received her B.S. in aerospace engineering from MIT in 2008. Following graduation, she served four years in the United States Air Force, spending most of her time as an operational flight test engineer on the F-35 Joint Strike Fighter. She received a PhD in Electrical and Computer Engineering from the University of Washington in 2019, where she studied the privacy, ethics, and policy of neural data. Her professional work experience includes Blue Origin, the ACLU of Washington, and a fellowship through TechCongress working on technology policy in the US House of Representatives. She also competes in triathlons and is the co-founder of the 501(c)3 Minority Veterans of America.

SpeakerBio: Jeff Rothblum, Founder at Plaintext Strategies

Jeff Rothblum, founder of Plaintext Strategies, has worked at the intersection of technology and policy for two decades. He has led government affairs at an AI startup, served as a cyber threat intelligence analyst, led cybersecurity policy the Senate Homeland Security and Governmental Affairs Committee, served as a Director of Cyber Policy and Plans at the White House Office of the National Cyber Director, and co-owned an artisan blacksmithing company.

SpeakerBio: Maurice Turner

Maurice Turner is a recognized public interest technologist and cybersecurity expert on the Public Policy team at TikTok. As a Technical Policy Lead, Turner plays a key role as a liaison collaborating between public policy and cross-functional teams to ensure understanding of cutting-edge technologies by non-technical audiences. He also advises the broader Americas public policy team on a wide range of technology, strategy, and policy issues.

SpeakerBio: Ayan Islam

Ayan Islam is an Adjunct Lecturer at American University School of Public Affairs' Cybersecurity Policy and Management program and cyber risk specialist at a Fortune 500 FinTech company. As former White House Director of Cyber Workforce, she served at the Office of National Cyber Director (ONCD) supporting the development and implementation of the National Cyber Workforce and Education Strategy. Previously, she was the Associate Policy Director for R Street's Cybersecurity and Emerging Threats team and contributed to special initiatives at the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA).

SpeakerBio: Beau Woods

No BIO available

Title: Finding Bugs Is Easy, Patching Isn't: Build Your Own Remediation Pipeline

Tags: Intermediate | AppSec Village | Creator Talk/Panel

When: Sunday, Aug 9, 11:50 - 12:20 PDT

Where: LVCCW Level 1 Hall 2 604 (Appsec Village) Main Stage - [Map](#)

Description:

AI made finding and exploiting bugs almost free. In one month, Anthropic's Project Glasswing surfaced over 10,000 high and critical bugs and patched fewer than 100. The maintainers on the receiving end are asking Anthropic to slow down, because they can't fix the bugs fast enough.

If one model can bury the world's best-funded security teams, what happens to the 1-to-5 person team with little security budget and a backlog now growing at machine speed?

This talk shows you how to build SPAR (Scan, Prioritize, Auto-fix, Rewrite): a remediation pipeline that chains call-graph reachability, EPSS percentiles, and SSVC decision logic into triage a small team can run, then routes the ones that matter through AI patch generation behind a regression-aware verification harness.

Speakers: Mohan Kumar, Naveen

SpeakerBio: Mohan Kumar

Mohan is a security leader with over a decade of experience in security architecture, engineering, and operations. He has a strong interest in developing robust security programs and a proven track record of creating proactive security roadmaps and strategies aligned with business objectives. He constantly seeks ways to elevate security processes and culture to the next level.

SpeakerBio: Naveen

Naveen is a Security Researcher with over 9 years of expertise specializing in AI, application, and cloud security. He invented 5 patents in Agentic Security space.

He possesses extensive knowledge in all aspects of product security, including threat modeling, DevSecOps, API security, and penetration testing. He is passionate about integrating security into the SDLC from design to deployment, ensuring the early detection and mitigation of vulnerabilities.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

DEF CON Talks - Friday - 12:30-13:30 PDT

Title: Fireside Chat with Gen. Paul Nakasone

Tags: DEF CON Official Talk

When: Friday, Aug 7, 12:30 - 13:30 PDT

Where: LVCCW Level 1 Hall 3 1006 (Main Track 1) - [Map](#)

Description:

Speakers: Paul Nakasone, Jeff "The Dark Tangent" Moss

SpeakerBio: Paul Nakasone

No BIO available

SpeakerBio: Jeff "The Dark Tangent" Moss

Mr. Moss is an internet security expert and is the founder of both the Black Hat Briefings and DEF CON Hacking conferences.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Five Million Industrial Control Systems Walk Into a Bar: What IRONMAP Found When It Scanned the Whole Internet

Tags: ICS Village | Creator Talk/Panel

When: Sunday, Aug 9, 10:00 - 10:30 PDT

Where: LVCCW Level 1 Hall 3 801 (Creator Stage 1) - [Map](#)

Description:

What does the global attack surface of operational technology actually look like at internet scale? We built IRONMAP, a purpose-built OT/ICS intelligence platform, to find out — and the answer is both larger and more disturbing than we expected.

Over the course of this ongoing research project, IRONMAP has catalogued over 5.5 million ICS/OT-facing assets across the public internet, with more than 2.25 million flagged as high-risk. Using deep protocol fingerprinting across all major industrial protocols — EtherNet/IP (CIP), Modbus TCP, Siemens S7, DNP3, IEC 60870-5-104, OPC-UA, BACnet/IP, Omron FINS, GE SRTP, Tridium Fox, and more — IRONMAP goes well beyond port scanning to perform authenticated protocol enumeration, live register reads, and tag harvesting using PLCDISCO, our multi-protocol OT scanner.

This talk presents a ground-level statistical portrait of the exposed OT internet: which protocols dominate, which sectors are most exposed, how vendor market share looks through the lens of deep insight and where in the world the highest concentrations of exposed critical infrastructure live (spoiler: it is not all China). We will walk through what over 242,000 EtherNet/IP devices look like when you enumerate their CIP identity objects, what ~500,000 Modbus devices expose in their holding registers, and what the live tag names of real PLCs tell you about what processes they are running.

We then turn to a specific and underappreciated issue: Automatic Tank Gauges (ATGs). IRONMAP found 149 confirmed ATG systems directly exposed to the internet, the majority of them Veeder Root TLS-350 and TLS-450 units — the dominant ATG platform at commercial fueling facilities across North America. These systems, reachable via the Guardian ASP protocol on TCP/10001, require no authentication on older firmware and respond to a simple serial-style command set with:

- Current fuel volume per tank, in gallons
- Product type (Unleaded, Premium, Diesel, Jet-A, Heating Oil)
- Live alarm states (high water, leak detection, low fuel, overfill)
- Delivery event history and timestamps
- Up to 8 tank probes per unit

The implications are significant. Exposed ATGs reveal not just that a facility has fuel storage, but how much, what kind, and when deliveries occur — operational patterns that are directly relevant to physical security and supply chain intelligence. IRONMAP discovered ATGs at locations that include commercial truck stops, bulk fuel terminals, and sites with product profiles consistent with aviation or military use. We will demonstrate a live walk-through of what an unauthenticated session reveals, discuss the responsible disclosure posture we have taken, and present mitigation guidance for asset owners.

Attendees will leave with a realistic, data-grounded view of the exposed OT landscape — not a cherry-picked set of scary screenshots, but statistically representative findings from a 5.5-million-asset dataset — plus actionable context on the ATG exposure class and how to find and fix it.

SpeakerBio: Matt Caldwell, Tophat Security

Matt Caldwell is the founder of Tophat Security, cyber security firm specializing in innovative OT/ICS software and tools, red team operations, and critical infrastructure research. With over a decade of experience in industrial control system security, Matt has assessed environments spanning oil and gas, electric utilities, water treatment, manufacturing, and federal government. He built IRONMAP as a research platform to continuously map the internet-exposed OT attack surface at scale, applying it to build threat intelligence, support disclosure efforts, and develop data-driven visibility into the global ICS

exposure problem. Matt holds relevant certifications in cyber security and penetration testing and has presented research at global OT/ICS security conferences. He is based in Athens, Georgia, and speaks regularly with asset owners, government stakeholders, and research organizations on OT exposure topics.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Fix It, Snooze It, or Ignore It? Cloud Security Decisions Under Pressure

Tags: Cloud Village | Creator Event/Activity | Strategic Defense

When: Saturday, Aug 8, 13:30 - 14:30 PDT

Where: LVCCW Level 3 W311 (Cloud Village Labs) B - [Map](#)

Description:

Cloud security teams rarely struggle to find issues. They struggle to decide what actually matters—and how to fix them with limited resources.

In this interactive CloudSec Village lab hosted by Aikido Security, attendees step into the role of a cloud security lead. Navigating a custom simulation dashboard, you'll manage a realistic environment spanning containers, Kubernetes, serverless, and virtual machines.

The catch? Your engineering teams have a strict cap on available hours, and every fix comes with an estimated time cost. You must evaluate a live queue of vulnerabilities, assign remediation to the right teams, and decide what to fix, defer, or ignore to find the most optimal defense strategy before your resources run out.

This drop-in lab focuses on real-world decision-making under pressure rather than theory. Join at any time, manage your clock, and see how your prioritization strategy compares.

SpeakerBio: Mackenzie Jackson

Mackenzie is the Field CTO for Aikido Security, helping tech leaders understand application security through an attacker's lens. As the co-founder and former CTO health tech company Conpago, he understands the challenges of building secure applications. He has spoken in over 30 countries, hosts the popular Podcast The Secure Disclosure, and contributes to multiple publications including Dark Reading, Financial Times, and Fast Company.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Aerospace Village - Sunday - 10:00-13:59 PDT

Title: Flight Simulator/EFB

Tags: Aerospace Village | Creator Event/Activity

When: Sunday, Aug 9, 10:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 2 700 (Aerospace Village) - [Map](#)

Description:

Experience the effects of tampered engine performance data as you take the controls on a departing flight. Feel for yourself how vulnerabilities in electronic flight bags can have a physical impact inside the cockpit.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Aerospace Village - Friday - 10:00-17:59 PDT

Title: Flight Simulator/EFB

Tags: Aerospace Village | Creator Event/Activity

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 2 700 (Aerospace Village) - [Map](#)

Description:

Experience the effects of tampered engine performance data as you take the controls on a departing flight. Feel for yourself how vulnerabilities in electronic flight bags can have a physical impact inside the cockpit.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Aerospace Village - Saturday - 10:00-17:59 PDT

Title: Flight Simulator/EFB

Tags: Aerospace Village | Creator Event/Activity

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 2 700 (Aerospace Village) - [Map](#)

Description:

Experience the effects of tampered engine performance data as you take the controls on a departing flight. Feel for yourself how vulnerabilities in electronic flight bags can have a physical impact inside the cockpit.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Flow Like Water: Experiences from Physical Red Teaming

Tags: Physical Security Village | Creator Talk/Panel

When: Friday, Aug 7, 12:00 - 12:30 PDT

Where: LVCCW Level 1 Hall 3 1104 (Creator Stage 4) - [Map](#)

Description:

Physical red teaming remains one of the most consequential and under-discussed disciplines in offensive security. While network intrusions dominate the conversation, a determined adversary at the perimeter can bypass millions of dollars in cyber defenses with a lanyard, a clipboard, and a confident smile. This talk distills lessons learned from real-world physical red team engagements that achieved their objectives, walking through the tactics, techniques, and tooling that consistently produced results across diverse target environments.

Topics include reconnaissance and target profiling, pretext development and social engineering at entry points, covert entry tooling (bypass devices, RFID cloning, lock and latch attacks), implant deployment for persistence, and methods for chaining physical access into network footholds. Emphasis is placed on what actually worked, not theoretical attack trees, alongside the operational considerations, failure modes, and decision points that separate a successful op from a burned one.

SpeakerBio: Michael "v3ga" Aguilar, Principal Consultant at Sophos Red Team

Michael Aguilar (v3ga) is a Principal Consultant on the Sophos Red Team, paid to think like the people his clients are afraid of. His work lives at the intersection of offensive security, vulnerability research, and low-level systems programming, Windows internals, reverse engineering, and the kind of dusty attack surfaces that nobody has looked at since the protocol was ratified. Sometimes, he's lucky enough to perform full Physical Red teams against his client targets. His method is unglamorous and effective: Analyze, Formulate, Target, Attack (covertly).

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Fooling Coding Agents for Fun and Profit

Tags: AI Village | Creator Talk/Panel

When: Friday, Aug 7, 14:00 - 14:59 PDT

Where: LVCCW Level 1 Hall 2 603 (AI Village) - [Map](#)

Description:

This is a sit down discussion in a more casual conversational format: Companies are increasingly deploying coding agents to triage bug reports, resolve support tickets, and open pull requests. These agents have direct access to codebases, CI/CD pipelines, internal tooling, and, often, the internet. These are exactly the conditions that make indirect prompt injection devastating.

This talk presents end-to-end vulnerability chains we have discovered and disclosed in real coding agents. We'll demo how adversary-controlled content (e.g., a bug report from a user) can hijack an agent's goal and lead to outcomes like source code exfiltration and malicious pull requests.

As coding agents become increasingly autonomous and interact with the outside world more frequently, these attacks will only grow more potent. We close with recommendations for how companies and codegen providers can defend against them.

Speakers: Matt Galligan, Jack Cable

SpeakerBio: Matt Galligan

Matt has spent his career on both sides of the fence: building deceptive cyber systems and the security automation behind one of the DOD's largest software factories, then joining CISA's Rapid Action Force — where the job was, more or less, "hack the entire federal government, daily," between vuln research and no-notice red team engagements. After a stint in big tech, he's now at Corridor focusing his efforts on building a rare thing in the industry: a security product that security teams actually love.

SpeakerBio: Jack Cable, CEO and Co-Founder at Corridor

Jack Cable is the CEO and Co-Founder of Corridor, the security layer for AI coding. Prior to that, Jack served as a Senior Technical Advisor at the Cybersecurity and Infrastructure Security Agency (CISA), where he helped lead the agency's Secure by Design initiative. Before CISA, Jack worked as a TechCongress Fellow for the Senate Homeland Security and Governmental Affairs Committee, advising Chairman Gary Peters on cybersecurity policy, including open source software security. He previously worked as a Security Architect at Krebs Stamos Group. Jack is a top bug bounty hacker, having identified over 350 vulnerabilities in hundreds of companies. After placing first in the Hack the Air Force bug bounty challenge, he began working at the Pentagon's Defense Digital Service. Jack studied computer science at Stanford University and has published academic research on election security, ransomware, and cloud security.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: For Prompt Injection, Press 1: Hacking AI Voice Agents

Tags: Social Engineering Community Village | Creator Talk/Panel

When: Saturday, Aug 8, 14:00 - 14:30 PDT

Where: LVCCW Level 3 W317-319 (Social Engineering Community Village) - [Map](#)

Description:

What happens when you social engineer an AI agent that was trained to be helpful over the phone? Can you get it to reveal its system prompt out loud? Will it disclose information about other callers? How far can you push it before its guardrails kick in? AI voice agents sit behind telephony layers like speech-to-text, text-to-speech, and call routing that introduce new attack surfaces and opportunities. They're replacing human operators everywhere: answering phones at doctors' offices, handling IT help desks, triaging customer support, and booking appointments. They sound human, but underneath, they're the same LLMs we've been prompt injecting. I built an open-source tool that tackles this by placing real phone calls to voice AI agents, speaking attack scenarios using text-to-speech, capturing responses via speech recognition, and analyzing transcripts for signs of successful exploitation. It maps 20 attack scenarios across five categories from the OWASP Top 10 for LLM Applications: prompt injection, sensitive information disclosure, system prompt leakage, excessive agency, and misinformation. Detection uses pattern matching and an LLM judge to catch both obvious and subtle failures.

SpeakerBio: Willie Zhang, Offensive Security Consultant

Willie Zhang is an Offensive Security Consultant with experience protecting companies by thinking like an attacker. What started as a \$1 online course on ethical hacking in college turned into a career built on finding the gaps in systems that aren't supposed to have any. Willie has a growing passion for understanding and attacking AI systems, building on a foundation of testing everything from corporate networks to the humans that run them. When he's not learning something new, Willie is in a League of Legends lobby, because apparently cybersecurity isn't chaotic enough.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Forcing Physical Interlocks into Data Transit and Storage Replication

Tags: Data Duplication Village | Creator Talk/Panel

When: Saturday, Aug 8, 12:15 - 12:45 PDT

Where: LVCCW Level 2 W203 (Data Duplication Village) - [Map](#)

Description:

Traditional software-based security cannot prevent data destruction or unauthorized cloning when authorized credentials are compromised. This presentation introduces a hardware-level physical intervention approach with a zero-OS FPGA architecture to overcome vulnerabilities at the L3/L4 layer. This invisible Layer-2 transparent bridge, lacking IP or MAC addresses, performs sub-nanosecond-level gate-level Deep Packet Inspection (DPI) on the pipeline. When high-risk storage commands (deletion, unauthorized data transfer, etc.) are detected at the silicon level, the data flow is hardware-intercepted and held in a "Catch-and-Release" buffer until a physical human confirmation is received.

Speakers: Mehmet Önder Key, Temel Demir

SpeakerBio: Mehmet Önder Key, Cyber Security Consultant

Önder Key is a cybersecurity consultant specializing in critical infrastructure security, zero-day vulnerability analysis, and offensive security. He has advised organizations in high-security sectors such as defense, aerospace, and finance, with hands-on experience in both red teaming and strategic security engineering. His work has been featured across numerous countries and platforms, contributing to the discovery of systemic vulnerabilities. Currently, he provides consultancy to TurkNet and continues to advance the global offensive security ecosystem by challenging traditional approaches to cybersecurity.

SpeakerBio: Temel Demir

Temel Demir is a cybersecurity researcher and hardware architect specializing in hardware defense, offensive security, and the protection of critical infrastructure. With a core focus on embedded system vulnerabilities and Layer-1/Layer-2 network manipulation, his research involves developing deterministic, hardware-enforced frameworks that bypass traditional software-defined security flaws. Having previously shared security research on global stages, his work bridges the gap between sophisticated threat actor methodologies and immutable physical security barriers.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Forcing Physical Interlocks into Data Transit and Storage Replication

Tags: Data Duplication Village | Creator Talk/Panel

When: Friday, Aug 7, 13:00 - 13:30 PDT

Where: LVCCW Level 2 W203 (Data Duplication Village) - [Map](#)

Description:

Traditional software-based security cannot prevent data destruction or unauthorized cloning when authorized credentials are compromised. This presentation introduces a hardware-level physical intervention approach with a zero-OS FPGA architecture to overcome vulnerabilities at the L3/L4 layer. This invisible Layer-2 transparent bridge, lacking IP or MAC addresses, performs sub-nanosecond-level gate-level Deep Packet Inspection (DPI) on the pipeline. When high-risk storage commands (deletion, unauthorized data transfer, etc.) are detected at the silicon level, the data flow is hardware-intercepted and held in a "Catch-and-Release" buffer until a physical human confirmation is received.

Speakers: Mehmet Önder Key, Temel Demir

SpeakerBio: Mehmet Önder Key, Cyber Security Consultant

Önder Key is a cybersecurity consultant specializing in critical infrastructure security, zero-day vulnerability analysis, and offensive security. He has advised organizations in high-security sectors such as defense, aerospace, and finance, with hands-on experience in both red teaming and strategic security engineering. His work has been featured across numerous countries and platforms, contributing to the discovery of systemic vulnerabilities. Currently, he provides consultancy to TurkNet and continues to advance the global offensive security ecosystem by challenging traditional approaches to cybersecurity.

SpeakerBio: Temel Demir

Temel Demir is a cybersecurity researcher and hardware architect specializing in hardware defense, offensive security, and the protection of critical infrastructure. With a core focus on embedded system vulnerabilities and Layer-1/Layer-2 network manipulation, his research involves developing deterministic, hardware-enforced frameworks that bypass traditional software-defined security flaws. Having previously shared security research on global stages, his work bridges the gap between sophisticated threat actor methodologies and immutable physical security barriers.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Forensics of Covert Entry

Tags: Physical Security Village | Creator Talk/Panel

When: Friday, Aug 7, 15:30 - 15:59 PDT

Where: LVCCW Level 1 Hall 3 1104 (Creator Stage 4) - [Map](#)

Description:

You know lockpicking. You know lock bypass. You might know evasion tactics for alarms and surveillance systems. But what traces get left behind if an attacker does these? This talk will give an introduction to the forensics of covert entry techniques - what marks get left behind, how to tell whether someone entered, when it happened, what tactics and tools were used, and what skill level the attacker had. Taught by two founding members of the Physical Security Village, this talk will also show the interesting and funny results when certain entry techniques are applied *thousands of times* on one door, which will tune your eye for spotting when it's only happened once.

Speakers: Bill Graydon, Bobby Graydon

SpeakerBio: Bill Graydon, GGR Security

Bill Graydon is a Principal at GGR Security, where he designs and evaluates security systems and building construction for a wide range of industries - including testing them on physical pen tests. Through this, he hacks everything from locks and alarms to critical infrastructure; this has given him some very fine-tuned skills for breaking stuff. He's passionate about advancing the security field through research, teaching numerous courses, giving talks, and running DEF CON's Lock Bypass Village. He's received various degrees in computer engineering, security, and forensics and comes from a broad background of work experience in cyber security, anti-money laundering, and infectious disease detection.

SpeakerBio: Bobby Graydon

Robert is an avid researcher of lock manipulation, picking, bypass, and other vulnerabilities to discover and evaluate possible flaws and methods of attack. He has a passion not only for hacking, but teaching as well, being one of the founders of Physical Security Village, and enjoys speaking at various physec engagements. He has well-honed skills, as well as a thorough understanding of the mechanics and function of many types of high security locks, allowing him to effectively search for and test methods of cracking high security systems.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Forged in fire: Malware Factory

Tags: OWASP Foundation | Creator Talk/Panel

When: Friday, Aug 7, 15:15 - 15:59 PDT

Where: LVCCW Level 1 Hall 3 1100 (Creator Stage 7) - [Map](#)

Description:

We are moving beyond prompt engineering into the era of Agentic Warfare. This session pulls back the curtain on a clandestine bridge between the OWASP community and the underground. We aren't here to lecture on "best practices." We are here to hand you the blueprints for the Forge.

The Agenda:

The Artisan's Edge: Weaponizing LLMs as high-bandwidth force multipliers for surgical, manual exploit crafting. Agentic Persistence: Engineering self-correcting, goal-oriented malware that adapts to environment constraints in real-time. Ghost Pipelines: Architecting air-gapped, invisible infrastructures for weapon synthesis where the trail ends before it begins. Monetizing the Machine: Scaling high-impact, client-side payloads for maximum "fun and profit."

OWASP has chapters in every major city—think of them as your local cells. We are opening the laboratory doors to the elite. If you have the craft, we have the infrastructure.

Come claim your seat in the Forge.

Speakers: Jon McCoy, Andra Lezza

SpeakerBio: Jon McCoy, Security Architect, OWASP

Software security architect, Jon McCoy brings over 20 years of experience in software development and cybersecurity to the forefront. With a strong foundation in .NET development, Jon transitioned into security, driven by a passion for proactive defense strategies and secure coding practices.

A dedicated contributor to the OWASP community, Jon has shared his expertise at numerous industry events, including OWASP Global AppSec. His recent presentation on "Lessons Learned from Past Security Breaches" highlighted critical takeaways for strengthening AppSec efforts before and after incidents.

SpeakerBio: Andra Lezza, Principal Application Security Specialist at Sage / OWASP Leader

Andra is a Principal Application Security Specialist at Sage, with over seven years of experience in the field of application security. She is responsible for implementing DevSecOps practices, conducting security assessments, and developing secure coding guidelines for software engineering and AI/ML teams. She has a strong background in software development and project management, as well as a master's degree in information and computer sciences. She has been co-leading the OWASP London Chapter since 2019, where she organises and delivers events and workshops on various security topics. She is passionate about educating and empowering developers and stakeholders to build and deliver secure software and best practices in a fast-paced, results-driven environment.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Forget FIPS: An Analysis of Russian and Chinese Cryptographic Standards

Tags: Crypto & Privacy Village | Creator Talk/Panel

When: Saturday, Aug 8, 14:00 - 14:59 PDT

Where: LVCCW Level 1 Hall 3 1102 (Creator Stage 6) - [Map](#)

Description:

Despite securing the connections of over a billion people, Russian and Chinese state cryptography often remains unfamiliar to western practitioners. We survey the GOST, ShangMi, and ZUC standards, their respective histories, designs, and the current academic understandings of their security. We additionally cover implementation conveniences, such as the use of AES-NI instructions with SM4 as a method of side channel hardening, and algorithmic peculiarities, such as the hidden substructure of the Kuznyechik and Streebog S-box. We conclude with considerations about why specific algorithms were standardized, and how they reflect the priorities of the respective nations that standardized them.

SpeakerBio: Infocalypse

Infocalypse is a GCC developer and cryptography enthusiast, with a particular focus on applied cryptography and implementation security. He has contributed to libstdc++-v3 and GCC's OpenMP implementation, authored cryptographic CTF challenges for C2 Society and the "?Cube" CTF, and has conducted security research leading to CVEs involving cryptographic aspects of Apache Druid and mbedTLS.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Forgotten but Not Gone: Unauthenticated RCEs and LPEs in Legacy Linux Services

Tags: DEF CON Official Talk | Demo | Tool | Exploit

When: Saturday, Aug 8, 11:00 - 11:59 PDT

Where: LVCCW Level 1 Hall 3 906 (Main Track 3) - [Map](#)

Description:

The cybersecurity community chases the greatest risks in the latest tech, while components with outdated security principles gather dust. Companies rush to secure their latest AI product, while their network remains the same. Do attackers really need more than legacy services to take you down?

We asked this question as we analyzed an unauthenticated RCE in GNU-TelnetD that was discovered in January. We were amazed a simple shell injection existed for so long in the most popular telnet daemon. We further investigated Telnet and discovered it runs a root-privileged process with environment variables supplied by an unauthenticated client! Leading us to a privilege escalation vulnerability.

We then looked into Samba, the Linux service for sharing files and printers over SMB. Focused on shell injections, we searched for command execution using format strings - and we couldn't believe it! Two more shell injection RCEs waited for us! In this talk, you'll ask yourself, "How come it was only found in 2026?!" We will analyze the unauthenticated RCE in TelnetD and reveal three severe vulnerabilities: 2 unauthenticated RCEs in Samba (CVE-2026-4480 & CVE-2026-4408) and a privilege escalation in TelnetD (CVE-2026-28372). The routers or printers you forget to update might run those services, and they put you at risk

<https://www.safebreach.com/blog/safebreach-labs-root-cause-analysis-and-poc-exploit-for-cve-2026-24061/>

SpeakerBio: Ron Ben Yizhak, SafeBreach

Ron (@RonB_Y) is a security researcher at SafeBreach with 11 years of experience. He works in vulnerability research and has knowledge in forensic investigations, malware analysis and reverse engineering. Ron previously worked in the development of security products and spoke several times at DEF CON

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: FORTRESS Framework

Tags: Physical Security Village | Creator Talk/Panel

When: Saturday, Aug 8, 13:30 - 13:59 PDT

Where: LVCCW Level 1 Hall 3 1104 (Creator Stage 4) - [Map](#)

Description:

As physical security threats increase in sophistication and frequency, organizations face a critical gap in their physical security, the lack of a structured framework for physical security assessments and tests. FORTRESS was designed to fill this need by providing a categorized model of physical Tactics, Techniques, and Procedures (TTPs), each aligned to industry-standard compliance controls such as NIST, HIPAA, FedRAMP, ISO 27001, and PCI DSS. Designed for both red and blue teams, FORTRESS enables coordinated, repeatable physical security testing by consolidating adversarial behaviors into mapped TTPs. Each TTP is supported by detailed guidance for the execution, validation, and reporting of physical security gaps making assessments more consistent across multiple teams, business units, and future engagements. This paper presents the overall breakdown of FORTRESS, highlighting its application, structure, and flow. I believe this framework fills that critical void in operational and physical security and can be viewed as the foundation for enhancing and maturing physical security risk programs with real threat models as the base.

SpeakerBio: Brad "SnoOose" Ammerman

Brad Ammerman, a leading figure in security testing, currently serves as the Senior Director at Prescient Security. His background includes influential roles at companies like Foresite, Optiv, Lockheed Martin, DIA, DoD, and Supreme Court of Nevada, where he developed his expertise in offensive security and team management. A skilled hacker himself, Brad is also a recognized speaker, educator, mentor, and disabled veteran, dedicated to teaching and protecting others.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Four Newbies Vs. An Insulin Pump. How Hard Can It Be?

Tags: Biohacking Village | Creator Talk/Panel

When: Friday, Aug 7, 10:00 - 10:45 PDT

Where: LVCCW Level 1 Hall 3 1104 (Creator Stage 4) - [Map](#)

Description:

Medical devices are becoming increasingly connected—and that includes devices responsible for keeping people alive. In this talk, we share our journey as four security students taking on the challenge of analyzing an insulin pump as relative newcomers to hacking medical devices. Motivated by curiosity, concern for patient safety, and personal stakes, we set out to explore how an attacker might approach such a system using only public information, basic wireless knowledge, and persistence.

Rather than presenting ourselves as experts, we focus on the learning process: how we approached an unfamiliar, safety critical system, how we performed threat modeling when the “failure mode” is a human body, and how we handled the many moments where everything stopped making sense. We’ll walk through what worked, what didn’t, and how critical thinking helped us move forward when we hit a wall.

By reflecting on where we started, where we are today, and what remains unexplored, this talk highlights the value of a beginner’s mindset when analyzing real world systems like medical devices. Our goal is not to sensationalize risk, but to show how accessible security research, done responsibly, can contribute to better understanding and safer technology.

Speakers: Birgitte Jordal, Julia Kucharska, Emilie Jørstad, Selma Jenker

SpeakerBio: Birgitte Jordal

We are four Norwegian women that hold a bachelor’s degree in Digital Infrastructure and Cybersecurity from NTNU. Our interests include CTFs, ethical hacking, and penetration testing, with experience in cloud infrastructure, secure networking, and threat analysis.

SpeakerBio: Julia Kucharska

No BIO available

SpeakerBio: Emilie Jørstad

No BIO available

SpeakerBio: Selma Jenker

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Radio Frequency Village - Friday - 13:30-14:25 PDT

Title: Fox Hunting - Finding Rogue Access Points in the CTF and in the Wild

Tags: Radio Frequency Village | Creator Talk/Panel

When: Friday, Aug 7, 13:30 - 14:25 PDT

Where: LVCCW Level 1 Hall 1 409 (Radio Frequency Village) - [Map](#)

Description:

What does the fox say? Turns out the fox says quite a lot, you just need to know how to listen! A "fox" is a hidden transmitter, in this case a WiFi access point. In this talk we'll go from basics to advanced fox hunting, covering: direction finding, antenna selection, channel scanning, refresh rate, remote sensors, mobile devices, staying stealthy so the fox never sees you, and working as a team. Not only is it a great DEFCON pastime, it's a real-world skill that lasts long after the con.

SpeakerBio: Eric Escobar, Sophos - Red Team Lead

Eric is a seasoned pentester and a Red Tech Lead at Sophos. On a daily basis he attempts to compromise large enterprise networks to test their physical, human, network and wireless security. He has successfully compromised companies from all sectors of business including: Healthcare, Pharmaceutical, Entertainment, Amusement Parks, Banking, Finance, Technology, Insurance, Military, Retail, Food Distribution, Government, Education, Transportation, Energy and Industrial Manufacturing.

His team consecutively won first place at DEF CON 23, 24, and 25's Wireless CTF, snagging a black badge along the way. Forcibly retired from competing in the Wireless CTF, he now helps create challenges!

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Foxveil: Cloud-Native Loader Tradecraft on Cloudflare, Netlify, and Discord

Tags: Cloud Village | Creator Talk/Panel

When: Sunday, Aug 9, 11:50 - 12:30 PDT

Where: LVCCW Level 3 W313 (Cloud Village Talks) - [Map](#)

Description:

Malware loaders used to advertise themselves with throwaway domains, fragile hosting, and obvious command-and-control infrastructure. Foxveil is a hard reset in loader tradecraft. Less attacker-owned infrastructure, less disk-heavy execution, fewer static clues, and more abuse of platforms defenders see every day. This newly documented loader stages payloads from our most trusted and favorite cloud-native tool chains: Cloudflare Pages, Netlify, and Discord attachments, executes shellcode largely in memory, establishes persistence through masqueraded Windows artifacts, and actively rewrites analysis-significant strings at runtime to make reverse engineering and static detection harder. Across two observed variants, Foxveil combines several pieces of modern tradecraft into one compact initial-stage loader. One variant spawns a fake svchost.exe and performs Early Bird APC injection into the target process before it fully resumes. Another pulls shellcode from Discord attachments and executes it through self-injection. Both stage follow-on payloads from trusted platforms, drop files into SysWOW64 under names designed to blend into normal Windows noise, and use runtime string mutation to corrupt keywords such as beacon, meterpreter, shellcode, and even fox itself. This talk walks through the full Foxveil infection chain, from staging and shellcode delivery to persistence and follow-on deployment, and examines what makes this loader part of a broader shift in attacker and malware tradecraft by comparing both variants. The real story is not just cloud-hosted staging. It is the emergence of a loader model that borrows trust instead of building infrastructure. Foxveil examines what modern initial-stage malware looks like when it is designed for rotation, ambiguity, and survival.

Speakers:Shani Kurtzberg,Zohar Buber

SpeakerBio: Shani Kurtzberg

Shani Kurtzberg is an XDR Team Lead at Cato Networks and member of Cato CTRL. She leads the Threat Intelligence and XDR Detection Engineering initiatives. Prior to Cato, Shani served in the Israeli Air Force (IAF) as a Security Analyst, leading SOC operations to protect critical systems. Shani holds a Master of Business Administration (M.B.A.) from Peres Academic Center, specializing in Marketing and Product Management.

SpeakerBio: Zohar Buber

Zohar Buber is a security analyst in Cato Research Labs at Cato Networks. He focuses on network protocol analysis and malicious traffic detection, specializing in threat identification using network-based methods. He previously worked at Radware, where he examined threats in the DDoS industry. Zohar holds B.A focused in Business Administration, Information System Analysis // Zohar Buber, zohar@devtalks.me

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Free Ham Radio License Exams

Tags: Event | Ham Radio Village

When: Friday, Aug 7, 13:00 - 15:59 PDT

Where: LVCCW Level 3 W314 (Ham Radio Meeting) - [Map](#)

Description:

Free ham radio exams return to DEF CON 34! Partake in this hacker “rite of passage” by getting your license at DEF CON, presented by the Ham Radio Village.

While anyone is able to listen in to amateur/ham radio transmissions, only those who have an amateur radio license are able to fully partake in the “oldest hacker hobby”. With your license, you’ll be authorized by the FCC to transmit up to 1,500W on designated frequencies, build/modify radios & antennas, and even administer your own exams! Additionally, having your ham radio license can improve your resume as it is a well-recognized proof of technical and regulatory knowledge when it comes to all things radio.

About The Exam

In the US there are 3 current levels of amateur radio license - Technician, General, and Amateur Extra. You can progress through the levels by taking a series of multiple-choice exams showing increasing breadth of knowledge. Most folks at DEF CON looking to become a ham take just the technician exam.

The technician exam is a 35 question, multiple choice exam. Questions come from from a *public* question pool of 400 questions. Because of that, the most popular way folks at DEF CON prepare is by reading through all 400 questions before the exam, and learning hands on once you get licensed. Many study resources exist - most people recommend ham.study.

Signing Up

Who may register for this testing session:

- Anyone with an interest in obtaining a new Amateur Radio license or upgrading their existing licenses.
- You may take multiple elements in a single appointment; we just ask that you have studied and are ready to pass.

Fees

- All license examinations administered by the Laurel VEC are free to all
- After passing, Laurel VEC will submit your application to the FCC. On acceptance you will receive an email from the FCC directly with instructions to pay the **\$35 application fee**.

Questions

If you have any questions leading up to DEF CON, come visit us on the Ham Radio Village Discord server (discord.gg/hrv) and let us know what questions you have. During the conference, come visit the Ham Radio Village to learn all things ham radio, including the studying, testing, and licensing process.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file



Title: Free Ham Radio License Exams

Tags: Event | Ham Radio Village

When: Sunday, Aug 9, 11:00 - 12:59 PDT

Where: LVCCW Level 3 W314 (Ham Radio Meeting) - [Map](#)

Description:

Free ham radio exams return to DEF CON 34! Partake in this hacker “rite of passage” by getting your license at DEF CON, presented by the Ham Radio Village.

While anyone is able to listen in to amateur/ham radio transmissions, only those who have an amateur radio license are able to fully partake in the “oldest hacker hobby”. With your license, you’ll be authorized by the FCC to transmit up to 1,500W on designated frequencies, build/modify radios & antennas, and even administer your own exams! Additionally, having your ham radio license can improve your resume as it is a well-recognized proof of technical and regulatory knowledge when it comes to all things radio.

About The Exam

In the US there are 3 current levels of amateur radio license - Technician, General, and Amateur Extra. You can progress through the levels by taking a series of multiple-choice exams showing increasing breadth of knowledge. Most folks at DEF CON looking to become a ham take just the technician exam.

The technician exam is a 35 question, multiple choice exam. Questions come from from a *public* question pool of 400 questions. Because of that, the most popular way folks at DEF CON prepare is by reading through all 400 questions before the exam, and learning hands on once you get licensed. Many study resources exist - most people recommend ham.study.

Signing Up

Who may register for this testing session:

- Anyone with an interest in obtaining a new Amateur Radio license or upgrading their existing licenses.
- You may take multiple elements in a single appointment; we just ask that you have studied and are ready to pass.

Fees

- All license examinations administered by the Laurel VEC are free to all
- After passing, Laurel VEC will submit your application to the FCC. On acceptance you will receive an email from the FCC directly with instructions to pay the **\$35 application fee**.

Questions

If you have any questions leading up to DEF CON, come visit us on the Ham Radio Village Discord server (discord.gg/hrv) and let us know what questions you have. During the conference, come visit the Ham Radio Village to learn all things ham radio, including the studying, testing, and licensing process.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file



Title: Free Ham Radio License Exams

Tags: Event | Ham Radio Village

When: Saturday, Aug 8, 11:00 - 16:59 PDT

Where: LVCCW Level 3 W314 (Ham Radio Meeting) - [Map](#)

Description:

Free ham radio exams return to DEF CON 34! Partake in this hacker “rite of passage” by getting your license at DEF CON, presented by the Ham Radio Village.

While anyone is able to listen in to amateur/ham radio transmissions, only those who have an amateur radio license are able to fully partake in the “oldest hacker hobby”. With your license, you’ll be authorized by the FCC to transmit up to 1,500W on designated frequencies, build/modify radios & antennas, and even administer your own exams! Additionally, having your ham radio license can improve your resume as it is a well-recognized proof of technical and regulatory knowledge when it comes to all things radio.

About The Exam

In the US there are 3 current levels of amateur radio license - Technician, General, and Amateur Extra. You can progress through the levels by taking a series of multiple-choice exams showing increasing breadth of knowledge. Most folks at DEF CON looking to become a ham take just the technician exam.

The technician exam is a 35 question, multiple choice exam. Questions come from from a *public* question pool of 400 questions. Because of that, the most popular way folks at DEF CON prepare is by reading through all 400 questions before the exam, and learning hands on once you get licensed. Many study resources exist - most people recommend ham.study.

Signing Up

Who may register for this testing session:

- Anyone with an interest in obtaining a new Amateur Radio license or upgrading their existing licenses.
- You may take multiple elements in a single appointment; we just ask that you have studied and are ready to pass.

Fees

- All license examinations administered by the Laurel VEC are free to all
- After passing, Laurel VEC will submit your application to the FCC. On acceptance you will receive an email from the FCC directly with instructions to pay the **\$35 application fee**.

Questions

If you have any questions leading up to DEF CON, come visit us on the Ham Radio Village Discord server (discord.gg/hrv) and let us know what questions you have. During the conference, come visit the Ham Radio Village to learn all things ham radio, including the studying, testing, and licensing process.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file



Title: Free IP, Free Chaos: DHCP-Assisted Flooding Against Automotive Ethernet

Tags: Car Hacking Village | Creator Talk/Panel

When: Saturday, Aug 8, 16:00 - 16:30 PDT

Where: LVCCW Level 1 Hall 3 801 (Creator Stage 1) - [Map](#)

Description:

Modern vehicles are increasingly adopting Automotive Ethernet for UDS-based diagnostics instead of CAN. While Gateway ECUs are designed to restrict communication to specific IPs, some support DHCP to facilitate communication with diagnostic tools. This DHCP support allows an attacker to deploy a rogue DHCP server via the OBD Ethernet interface, assigning a controlled IP to the Gateway ECU and enabling network-level attacks without any prior knowledge of the vehicle's internal network. In this talk, we demonstrate that high-rate Layer 2/3 flooding — regardless of protocol (ARP, ICMP, UDP, TCP) — disrupts safety-critical systems including AVN, wipers, headlights, and causes abrupt stopping when shifted into Drive or Reverse, and that at higher packet rates the infotainment display blacks out and does not recover until fully powered down. We discovered these findings on a production vehicle and have prepared a demo.

SpeakerBio: Yehyeong Lee, Autocrypt Inc.

Yehyeong Lee is a cybersecurity engineer specializing in automotive security and embedded systems. He focuses on vulnerability analysis and penetration testing of vehicle ECUs and in-vehicle networks. His work includes real-world vehicle security testing and automotive network attacks. His research interests include automotive security, firmware analysis, and embedded system security.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Social Gatherings/Events - Sunday - 12:00-12:59 PDT

Title: Friends of Bill W

Tags: Meetup

When: Sunday, Aug 9, 12:00 - 12:59 PDT

Where: LVCCW Level 3 W301 (Misc Meeting Room) - [Map](#)

Description:

We know DEF CON and Vegas can be a lot. If you're a friend of Bill W who's looking for a meeting or just a place to collect yourself, DEF CON 34 has you covered. Join us throughout the conference in room W301. Meetings will be Thursday, Friday, Saturday, and Sunday.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Social Gatherings/Events - Thursday - 12:00-12:59 PDT

Title: Friends of Bill W

Tags: Meetup

When: Thursday, Aug 6, 12:00 - 12:59 PDT

Where: LVCCW Level 3 W301 (Misc Meeting Room) - [Map](#)

Description:

We know DEF CON and Vegas can be a lot. If you're a friend of Bill W who's looking for a meeting or just a place to collect yourself, DEF CON 34 has you covered. Join us throughout the conference in room W301. Meetings will be Thursday, Friday, Saturday, and Sunday.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Social Gatherings/Events - Thursday - 17:00-17:59 PDT

Title: Friends of Bill W

Tags: Meetup

When: Thursday, Aug 6, 17:00 - 17:59 PDT

Where: LVCCW Level 3 W301 (Misc Meeting Room) - [Map](#)

Description:

We know DEF CON and Vegas can be a lot. If you're a friend of Bill W who's looking for a meeting or just a place to collect yourself, DEF CON 34 has you covered. Join us throughout the conference in room W301. Meetings will be Thursday, Friday, Saturday, and Sunday.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Social Gatherings/Events - Friday - 12:00-12:59 PDT

Title: Friends of Bill W

Tags: Meetup

When: Friday, Aug 7, 12:00 - 12:59 PDT

Where: LVCCW Level 3 W301 (Misc Meeting Room) - [Map](#)

Description:

We know DEF CON and Vegas can be a lot. If you're a friend of Bill W who's looking for a meeting or just a place to collect yourself, DEF CON 34 has you covered. Join us throughout the conference in room W301. Meetings will be Thursday, Friday, Saturday, and Sunday.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Social Gatherings/Events - Friday - 17:00-17:59 PDT

Title: Friends of Bill W

Tags: Meetup

When: Friday, Aug 7, 17:00 - 17:59 PDT

Where: LVCCW Level 3 W301 (Misc Meeting Room) - [Map](#)

Description:

We know DEF CON and Vegas can be a lot. If you're a friend of Bill W who's looking for a meeting or just a place to collect yourself, DEF CON 34 has you covered. Join us throughout the conference in room W301. Meetings will be Thursday, Friday, Saturday, and Sunday.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Social Gatherings/Events - Saturday - 12:00-12:59 PDT

Title: Friends of Bill W

Tags: Meetup

When: Saturday, Aug 8, 12:00 - 12:59 PDT

Where: LVCCW Level 3 W301 (Misc Meeting Room) - [Map](#)

Description:

We know DEF CON and Vegas can be a lot. If you're a friend of Bill W who's looking for a meeting or just a place to collect yourself, DEF CON 34 has you covered. Join us throughout the conference in room W301. Meetings will be Thursday, Friday, Saturday, and Sunday.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Social Gatherings/Events - Saturday - 17:00-17:59 PDT

Title: Friends of Bill W

Tags: Meetup

When: Saturday, Aug 8, 17:00 - 17:59 PDT

Where: LVCCW Level 3 W301 (Misc Meeting Room) - [Map](#)

Description:

We know DEF CON and Vegas can be a lot. If you're a friend of Bill W who's looking for a meeting or just a place to collect yourself, DEF CON 34 has you covered. Join us throughout the conference in room W301. Meetings will be Thursday, Friday, Saturday, and Sunday.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Misc - Sunday - 12:00-12:59 PDT

Title: Friendship Bracelets

Tags: Women in Security and Privacy (WISP) | Creator Event/Activity

When: Sunday, Aug 9, 12:00 - 12:59 PDT

Where: LVCCW Level 1 Hall 4 1303 (Women in Security and Privacy (WISP) Community) - [Map](#)

Description:

Create a custom bracelet to wear or trade, each featuring a special bead with a hidden message or symbol of empowerment. This tactile, low-key activity is perfect for starting conversations and forming connections across the community. No crafting experience needed, just good vibes and open hands. Join us during this hour for a WISP bead to add to your bracelet (while supplies last)!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Misc - Friday - 12:00-12:59 PDT

Title: Friendship Bracelets

Tags: Women in Security and Privacy (WISP) | Creator Event/Activity

When: Friday, Aug 7, 12:00 - 12:59 PDT

Where: LVCCW Level 1 Hall 4 1303 (Women in Security and Privacy (WISP) Community) - [Map](#)

Description:

Create a custom bracelet to wear or trade, each featuring a special bead with a hidden message or symbol of empowerment. This tactile, low-key activity is perfect for starting conversations and forming connections across the community. No crafting experience needed, just good vibes and open hands. Join us during this hour for a WISP bead to add to your bracelet (while supplies last)!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Misc - Saturday - 12:00-12:59 PDT

Title: Friendship Bracelets

Tags: Women in Security and Privacy (WISP) | Creator Event/Activity

When: Saturday, Aug 8, 12:00 - 12:59 PDT

Where: LVCCW Level 1 Hall 4 1303 (Women in Security and Privacy (WISP) Community) - [Map](#)

Description:

Create a custom bracelet to wear or trade, each featuring a special bead with a hidden message or symbol of empowerment. This tactile, low-key activity is perfect for starting conversations and forming connections across the community. No crafting experience needed, just good vibes and open hands. Join us during this hour for a WISP bead to add to your bracelet (while supplies last)!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: From al-Kindi to DEF CON: The Middle Eastern and African Roots of Cybersecurity

Tags: Middle Easterns & Africans in Cyber Security (MEACS) | Creator Talk/Panel

When: Saturday, Aug 8, 10:00 - 10:59 PDT

Where: LVCCW Level 1 Hall 4 1306 (Middle Easterns & Africans in Cyber Security (MEACS) Community) - [Map](#)

Description:

The word algorithm comes from a mathematician in ninth-century Baghdad. The first person to write down how to break a cipher was working in the Arab world more than a thousand years before modern computing. The foundations of the field we now call cybersecurity were laid by scholars from the Middle East and Africa, and that lineage runs straight through to the practitioners in this room. This session opens the MEACS Community Space with a look at those roots, from the origins of cryptanalysis and algebra to the engineers, defenders, and founders carrying the work forward today. We will talk about where we come from, why representation in this field is not a side conversation, and what this community is here to build over the next few days. Whether you trace your roots to the region or you just want the history the industry skipped, you are welcome here. Come meet the people who make this space what it is.

Speakers: Amber Bennoui, Ezz Tahoun

SpeakerBio: Amber Bennoui

No BIO available

SpeakerBio: Ezz Tahoun

Ezz Tahoun is an award-winning cybersecurity data scientist recognized globally for his innovations in applying AI to security operations.

He has keynoted, trained & presented at BlackHat US, Sector, MEA, Asia & EU, DEFCON, SANS Summits, all the top Bsides, Securityweek ICS Conference and GISEC among many others.

His groundbreaking work earned him a gold edison award and accolades from Yale, Princeton, Northwestern, NATO, Microsoft, and Canada's CSE.

At 19, Ezz began his PhD in Computer Sci at the Univ of Waterloo, quickly gaining recognition through over 20 influential papers and open-source tools.

His experience includes leading advanced AI security ops projects for Orange CyberDefense, Forescout, RBC, and Huawei US.

He holds certifications such as GIAC Advisory Board, aCCISO, CISM, CRISC, GCIH, CEH, PMP and GCP-Cloud Architect, and served as an adjunct professor in cyber defense and warfare.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: From Application Telemetry Exposure to Cross-Service Pivoting and Full Azure Tenant Takeover

Tags: Red Team Village | Misc

When: Friday, Aug 7, 12:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 1 309 (Red Team Village) Tactic Table 2 - [Map](#)

Description:

Cloud-native teams often treat web app "config leaks," verbose telemetry, and CI/CD misconfigurations as separate, low-impact issues. This talk shows how those assumptions break in practice. We present a full kill chain where a single exposed Application Insights key in a front-end patient portal is chained with realistic but common Azure misconfigurations to achieve complete tenant compromise and Global Administrator access.

Starting from an exposed Application Insights Instrumentation Key in client-side JavaScript, we demonstrate how an attacker can pivot into the Application Insights query API, mine telemetry for over-privileged SAS URLs, and use those tokens to harvest sensitive data from Blob Storage and Storage Queues. We then show how seemingly innocuous Function App endpoints, intended for document ingestion, can be abused via SSRF and URL-based command injection to access local files and environment variables, recovering additional credentials. Finally, we weaponize misconfigured Azure DevOps pipelines and Library Variable Groups to exfiltrate cloud credentials to a webhook, escalate privileges in Entra ID, and take control of production workloads.

Rather than introducing a single novel vulnerability, this session focuses on the combinatorial risk of real-world misconfigurations across Application Insights, Storage, Functions, DevOps, and identity. Attendees will walk away with concrete cloud hunting techniques, a step-by-step attack chain they can reproduce in their own labs, and a prioritized remediation playbook for breaking similar chains in their environments.

Speakers:Chirag Savla,Raunak "Trouble1" Parmar

SpeakerBio: Chirag Savla

Chirag Savla is a cyber security professional with 10+ years of experience. His areas of interest include penetration testing, red teaming, azure and active directory security, and post-exploitation research. For fun, he enjoys creating open-source tools and exploring new attack methodologies in his leisure. Chirag has worked extensively on Azure, Active Directory attacks and defense, and bypassing detection mechanisms. He is the author of multiple open source tools such as Process Injection, Callidus, and others. He has presented at many conferences and local meetups and has trained people in international conferences like Blackhat, BSides Milano, Wild West Hackin' Fest, HackSpaceCon and VulnCon.

SpeakerBio: Raunak "Trouble1" Parmar

Raunak Parmar works as a senior cloud security engineer at White Knight Labs with 6+ years of experience. His areas of interest include web penetration testing, Azure/AWS security, source code review, scripting, and development. He enjoys researching new attack methodologies and creating open-source tools that can be used during cloud red team activities. He has worked extensively on Azure and AWS and is the author of Vajra, AzDevRecon and MsCodePhish. He has spoken at multiple respected security conferences like Black Hat, Defcon, Nullcon, RootCon, HackspaceCon, NorthSec, LeHack , etc and also at local meetups.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: From Buffer Overflow to Blackout: Chaining Attacks Against Industrial Systems

Tags: Red Team Village | Misc

When: Sunday, Aug 9, 12:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 1 309 (Red Team Village) Tactic Table 2 - [Map](#)

Description:

This presentation takes a practical, demo-driven approach to exploitation, demonstrating how a buffer overflow vulnerability can still serve as an entry point to compromise modern industrial infrastructures. The session is approximately 90% hands-on and 10% theoretical. The talk walks through the full attack chain, starting from initial exploitation and progressing to the development and execution of multistage shellcode. This shellcode establishes communication with a remote Command and Control (C2) server, retrieves an additional payload, and executes it directly in memory, bypassing traditional detection mechanisms. Once the environment is compromised, the session demonstrates how an attacker can gain full remote control, enabling command execution, lateral movement, and exfiltration of sensitive data, including critical assets such as licenses and proprietary industrial information. The talk also includes interaction with real-world devices such as RTUs (Remote Terminal Units), showing how malicious actions can directly impact industrial operations. In critical scenarios, this can lead to disruptions in essential services, including failures in energy systems and potential blackouts. The content is based on real-world pentesting experience conducted in an energy sector company in Brazil, providing a practical and applied perspective on risks in ICS/SCADA environments. The goal is to demonstrate how modern attacks combine vulnerabilities with advanced techniques, reinforcing the need for robust security strategies to protect critical infrastructure.

Speakers: Fernando Mengali, Thiago Cunha da Silva

SpeakerBio: Fernando Mengali, Information Security Specialist

Cybersecurity researcher focused on Pentesting and AppSec, also serving as a Practical / Hands-on Speaker. He also dedicates part of his research to critical infrastructure security (ICS/SCADA), exploring the intersection between classic vulnerabilities and industrial environments. He has over 18 years of experience in offensive security and practical application exploitation.

He has participated in research and development projects focused on vulnerability exploitation and offensive security.

Specialized in 0day discovery and exploit development, he has over 135 published CVEs and is ranked in the Top 10 contributors on VulDB <https://vuldb.com/users.top>.

Additionally, he has published multiple exploits and technical papers publicly available <https://www.exploit-db.com/?author=12136> and <https://packetstorm.news/files/author/8470/1>.

His work focuses on real-world vulnerability exploitation, including advanced scenarios such as memory corruption, buffer overflows, and complex environments.

He is the creator of <https://yrprey.com>, an educational framework that brings together more than 20 vulnerable applications based on the OWASP Top 10, used for practical training in Application Security and Offensive Security <https://owasp.org/www-project-vulnerable-web-application-directory>.

He is also the driving force behind <https://speakfy.io>, a project focused on promoting Information Security events globally.

Furthermore, he develops application security-oriented tools, such as <https://leapfix.co> (static code analysis) and <https://fitoxs.com>, a dynamic application analysis platform powered by artificial intelligence.

SpeakerBio: Thiago Cunha da Silva

Thiago Cunha is an offensive security specialist, or as he likes to put it: “professionally paid to break into systems before someone less friendly does.”

He currently works as a Red Team and Threat Intelligence Consultant at Banco Carrefour and as an instructor at the Kryfal, teaching future ethical hackers not to click on suspicious links.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Noob Community - Sunday - 11:00-12:59 PDT

Title: From Command Line to Center Stage: Hack Your Way to Confident Speaking

Tags: Noob Community | Creator Workshop

When: Sunday, Aug 9, 11:00 - 12:59 PDT

Where: LVCCW Level 1 Hall 4 1417 (Noob Community) - [Map](#)

Description:

Led by a seasoned security speaker with over 600 presentations under their belt and training from world-class Toastmasters, this interactive session completely bypasses the fluff to focus entirely on real-world delivery. This workshop is your chance to turn stage fright into stage might, equipping you with the tools to present with poise, project authority, and own the room.

SpeakerBio: James McQuiggan

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: From commit to compromise: securing the full pipeline with AI-assisted remediation

Tags: AppSec Village | Creator Talk/Panel | All Audiences

When: Sunday, Aug 9, 10:30 - 10:59 PDT

Where: LVCCW Level 1 Hall 2 604 (Appsec Village) Main Stage - [Map](#)

Description:

Most vulnerabilities aren't found because teams lack tools they persist because the cost of fixing them is too high. A finding without a concrete, context-aware fix is just noise developers learn to ignore. This talk walks through three real-world attack scenarios a secret leaked into git history, a compromised dependency in a supply chain attack, and an injection vulnerability introduced in a PR and shows how each is detected, mapped to OWASP Top 10:2025, and automatically remediated using AI running entirely on local infrastructure. No source code leaves the machine. The AI receives the vulnerable code block, CWE identifier, CVSS score, and OWASP category and returns a fix that is specific, correct, and ready to apply. Attendees leave with a working open-source tool and a new mental model for what AppSec remediation can look like.

SpeakerBio: Filipi Pires, Head of Technical Advocacy at SCYTHE

I've been working as Head of Technical Advocacy at SCYTHE, Founder & Investor at CROSS-INTEL, Advisor & Investor at Sherlockeye, BSides Porto Organizer, Red Team Village Director (DEF CON), Senior Advisor Raices Cyber Academy, Founder of Red Team Community (Brazil and LATAM), AWS Community Builder, Snyk Ambassador, Application Security Specialist and Hacking is NOT a crime Advocate. International Speaker at Security and New technologies events in many countries such as US (Black Hat & Defcon), Canada, France, Spain, Germany, Poland, Black Hat MEA - Middle-East - and others, I've served as University Professor in Master Degree in Portugal, Graduation and MBA courses at Brazilian colleges, in addition, I'm Creator and Instructor of the Course - Malware Attack Types with Kill Chain Methodology (PentestMagazine), PowerShell and Windows for Red Teamers(PentestMagazine) and Malware Analysis - Fundamentals (HackerSec).

Black Hat US 2025 - <https://blackhat.com/us-25/arsenal/schedule/presenters.html#filipi-pires-46329> Black Hat US 2024 - <https://blackhat.com/us-24/arsenal/schedule/presenters.html#filipi-pires-46329> Black Hat MEA 2025 - <https://blackhatmea.com/speaker/filipi-pires-0> Black Hat MEA 2024 - <https://blackhatmea.com/speaker/filipi-pires> DEF CON 33 / 32 - <https://sessionize.com/filipi-pires/> DEF CON - Adversary Village - <https://adversaryvillage.org/adversary-events/DEFCON-33/Filipi-Pires/>

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: From Dashboard to Exploit: Weaponizing and Winning the Cloud Queue

Tags: Cloud Village | Creator Event/Activity | Strategic Defense

When: Friday, Aug 7, 16:00 - 17:59 PDT

Where: LVCCW Level 3 W311 (Cloud Village Labs) B - [Map](#)

Description:

Finding a vulnerability on a dashboard is only half the battle. Knowing how an attacker will weaponize it is what separates great security engineers from the rest.

In this hands-on CloudSec Village lab hosted by Aikido Security, you will step into the shoes of both defender and attacker. Navigating a custom simulation dashboard, you'll face live vulnerabilities hidden across containerized apps and serverless functions. Your mission: don't just trust the scanner. You will dive into live mini-applications, execute real-world exploits to prove their impact, and see exactly how they register on the platform. This drop-in lab bridges the gap between passive triage and active offensive security — join any time and validate threats like a pro.

SpeakerBio: Mackenzie Jackson

Mackenzie is the Field CTO for Aikido Security, helping tech leaders understand application security through an attacker's lens. As the co-founder and former CTO health tech company Conpago, he understands the challenges of building secure applications. He has spoken in over 30 countries, hosts the popular Podcast The Secure Disclosure, and contributes to multiple publications including Dark Reading, Financial Times, and Fast Company.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: From Disclosure to Defense: Rebuilding Vulnerability Management for the AI Era

Tags: Policy @ DEF CON | Creator Talk/Panel

When: Saturday, Aug 8, 14:30 - 15:30 PDT

Where: LVCCW Level 2 W210-211 (Policy Village) - [Map](#)

Description:

AI has upended vulnerability discovery. What used to be scarce is now abundant: vulnerabilities can be found faster, at greater scale, and across more systems than ever before. Systems that uplevel vuln hunters are becoming widely available, to both defenders and malicious actors. Finding vulnerabilities used to be the hard part - but it's not anymore, and we need to adapt the vulnerability ecosystem to reflect that. But vulnerability management - thoughtful and methodical disclosure, triage, patching, and policy - still operates on assumptions of scarcity. That mismatch is becoming dangerous. If AI makes vulnerability discovery effectively infinite, what does a safe, scalable system for handling them actually look like? This panel will discuss how the vulnerability needs to evolve to match the moment. Current policy approaches - especially those mandating rapid reporting or broad sharing of unmitigated vulnerabilities - risk making systems less secure in an AI-driven environment. At the same time, rapid response by defenders is critical, and resources are scarce. Disclosure models need to evolve, governments need to support defenders, and incentives must align to ensure that AI-driven discovery strengthens security.

Speakers: Lindsey Cerkovnik, John Banghart, Ben Flatgard, Elizabeth Eigner

SpeakerBio: Lindsey Cerkovnik, CISA

Lindsey Cerkovnik is the Chief of CISA's Vulnerability Response & Coordination (VRC) Branch. Her team is responsible for CISA's Coordinated Vulnerability Disclosure (CVD) process, the Known Exploited Vulnerabilities (KEV) catalog, and CISA's Stakeholder Specific Vulnerability Categorization (SSVC) process. Lindsey and her team help to maintain, support, and advance the global vulnerability ecosystem by funding and overseeing the CVE and CVE Numbering Authority (CNA) programs, leading the production and dissemination of machine-readable vulnerability enrichment information, and engaging in valuable technical collaboration with the vulnerability research community.

SpeakerBio: John Banghart, Center for Cybersecurity Policy & Law

John Banghart leverages his significant federal government and private sector experience in cybersecurity to navigate issues related to risk management, government policy, standards and regulatory compliance, and incident management. He has successfully led efforts to address significant and high-profile cybersecurity issues within major government programs and institutions while facing complex legal, technical, and political circumstances. From 2013 to 2015, John played a key role in developing the Obama administration's cybersecurity and technology policy as the National Security Council's director for federal cybersecurity. He led policy, technical, and process efforts to reduce cybersecurity risk and improve metrics and measurement for all civilian, military, and intelligence community agencies. He served as a primary advisor on cybersecurity incidents and preparedness and led the National Security Council's efforts to address significant cybersecurity incidents, including those at OPM and the White House, among others. He also spent several years at the National Institute of Standards and Technology (NIST), both as a cybersecurity researcher and in the Office of the Undersecretary of Commerce for Standards and Technology. John also worked as a senior cybersecurity advisor for the Centers for Medicare and Medicaid Services, providing leadership to the cybersecurity preparations for the Healthcare.gov website.

SpeakerBio: Ben Flatgard, JPMorgan Chase

Ben Flatgard is an Executive Director with JPMorgan Chase Co. He leads public policy development and advocacy, as well as partnership initiatives, to improve the cybersecurity of the firm, its customers and clients, and the broader digital ecosystem. Ben previously served in the Obama Administration from 2009-2017. In his most recent post as Director for Cybersecurity

Policy on the National Security Council, Ben was responsible for leading cybersecurity policy development related to protection of critical infrastructure and emerging technologies. Before joining the National Security Council, Ben served as Senior Advisor to the Assistant Secretary of the Treasury for Financial Institutions. Prior to his time at Treasury, Ben held positions at the Department of Commerce and the White House. Ben graduated from the University of Edinburgh. He holds fellowships at the Atlantic Council in Washington, DC, and at the University of Sydney.

SpeakerBio: Elizabeth Eigner, Microsoft

Elizabeth Eigner is a Senior Manager on Microsoft's Global Cybersecurity Policy team, where she leads Microsoft's vulnerability policy portfolio, overseeing efforts to develop and implement strategies that address vulnerability management both in the United States and globally. She represents Microsoft on the Hacking Policy Council, where she works collaboratively with industry leaders and policymakers to advance responsible cybersecurity and strengthen the frameworks that underpin software security worldwide. Elizabeth also leads initiatives aimed at creating and enhancing national cyber strategies in countries around the world. She works closely with governments and stakeholders to strengthen policy frameworks and promote resilient cybersecurity practices globally. Elizabeth also leads Microsoft's Advancing Regional Cybersecurity (ARC) initiative, focusing on improving incident response capabilities and cyber capacity building in the Global South. Previously, she served as Microsoft's representative on the Cloud Service Provider Advisory Board (CSP-AB), contributing to FedRAMP public policy discussions and best practices for cloud security. Before joining Microsoft, Elizabeth worked at The Washington Technology Industry Association to enhance Washington State's innovation ecosystem. At MIT Solve, she collaborated with tech-based social entrepreneurs on solutions fostering digital inclusion and equitable economic opportunity. She holds a B.S. in Political Science from Northeastern University, with concentrations in Law and International Security.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: From Disk Image to ATT&CK in One Binary — a Reference Architecture for Modern Incident Response (in Rust)

Tags: LOONG Community | Creator Talk/Panel

When: Friday, Aug 7, 12:00 - 12:59 PDT

Where: LVCCW Level 1 Hall 3 1100 (Creator Stage 7) - [Map](#)

Description:

A Reference Architecture for Modern Incident Response (in Rust)

Incident response still runs on a toolbox: a dozen single-purpose parsers, a pile of CSVs, a timeline stitched together by hand, and a senior analyst's memory holding it all together. Every engagement re-solves the same plumbing. Every new artifact means a new script. And the hard-won expertise — how to read a prefetch run-count, how to resolve a ControlSet in an offline hive, which event IDs actually matter — lives in people, not in code you can run twice.

This talk argues for a different shape: incident response as a framework, not a toolbox — and backs the argument with a working reference implementation, Issen, an open-source DFIR engine written in Rust. You point Issen at evidence — an E01/EWF/VMDK or raw disk image, a memory dump — and it returns a single normalized timeline and an ATT&CK-mapped report. One static binary. No Python runtime, no agent, no cloud. It runs the same on an examiner's laptop, in CI, or inside a sealed evidence enclave.

Under the hood, Issen is deliberately thin. The real work lives in a fleet of standalone, single-responsibility forensic libraries — each a deep expert in one artifact family (NTFS and the change journal, registry hives, prefetch, SRUM, browser history, EVTX, SQLite, Windows and Linux memory) — that know nothing about each other. Issen is the orchestration and correlation layer that wires them into one story and speaks one normalized vocabulary of findings ("consistent with," never a verdict), each tagged to MITRE ATT&CK. We'll walk the layered model that makes this composition work — container filesystem / memory / log parser orchestration — and why every parser is medium-agnostic by design.

The most useful — and least glamorous — lesson is the one the talk is really about: capability is cheap to build and expensive to wire. Demonstrated live against the public "Stolen Szechuan Sauce" case, we'll show artifacts that were completely correct in isolation yet invisible end-to-end, because a decoder existed but nothing called it, or a file was extracted but never classified, or a real-world quirk (offline hives have no CurrentControlSet; large registry values are split into "big data" segments) quietly returned nothing. We'll trace each from "zero results" to ground truth.

Engineering substance throughout: panic-free, forbid(unsafe) parsers that treat every input as hostile; correctness validated against independent external oracles (not just the authors' own fixtures); and a clean separation between observed fact, forensic inference, and the conclusions that belong to a human, not a tool.

You'll leave with: a concrete, composable architecture for an IR pipeline you can adopt or fork; a working open-source reference to start from today; a repeatable method for finding "dark" capability in your own tooling; and a sober view of what to automate, what to keep human, and how to phrase findings so they survive scrutiny.

SpeakerBio: HUI Kwun Tai, Albert (4n6h4x0r), DC852

Albert Hui (@4n6h4x0r) is a digital forensics and incident response practitioner and the founder of Security Ronin. He builds open-source forensic tooling — including Issen, a Rust DFIR engine, and a family of panic-free libraries spanning disk, memory, registry, and application artifacts — and works hands-on as an examiner and expert witness testifying before courts of law, where findings have to survive cross-examination, not just look good on a slide. He's drawn to tooling an analyst can actually run twice: reproducible, offline, and honest about the line between observed fact and inference. In a past life he was an IBM Global Security Architect and a Deloitte Risk Advisory Director — which goes some way to explaining his propensity for horizontal thinking.



Title: From Findings to Remediations: Open Source Cloud Security at AI Speed with Prowler

Tags: Cloud Village | Creator Event/Activity | Strategic Defense

When: Saturday, Aug 8, 11:00 - 12:59 PDT

Where: LVCCW Level 3 W311 (Cloud Village Labs) B - [Map](#)

Description:

Cloud security teams are drowning in findings, but isolated misconfigurations rarely tell the full story. This hands-on workshop shows how to use Prowler, the open-source cloud security platform, to detect vulnerabilities and misconfigurations, prioritize risks, and remediate with AI- driven workflows. Participants will learn how to run Prowler from the CLI and import findings into Prowler Cloud using the new Import Findings workflow. From there, the workshop will go beyond traditional compliance reporting and demonstrate Prowler's newer capabilities: Attack Paths for graph- based analysis of cloud resources, permissions, findings, and privilege-escalation chains; Lighthouse AI for natural-language investigation, environment-aware prioritization, and direct guided remediation grounded in Prowler Hub's deterministic database; and the Prowler Claude Code plugin/MCP workflow for bringing security triage, remediation guidance, automated pull- request generation from IaC scanner findings as well as live cloud scans, and re-scanning into the developer workflow. By the end, attendees will understand how to use Prowler not only to assess compliance against frameworks such as CIS, GDPR, HIPAA, and cloud security best practices, but also to identify which findings matter most, explain their blast radius, and accelerate remediation with open source tooling and controlled AI assistance.

Speakers: Toni de la Fuente, Amit Sharma

SpeakerBio: Toni de la Fuente

Toni de la Fuente, Prowler's open-source creator and CEO, has profoundly impacted cybersecurity. His AWS background and passion for FLOSS, cloud computing, and information security have fueled contributions to projects such as phpRADmin and Alfresco BART. An esteemed speaker at Black Hat and DEF CON, de la Fuente champions open-source solutions and advancements in cloud security.

SpeakerBio: Amit Sharma

Amit Sharma has over a decade of experience as a cloud architect and built cybersecurity and observability products at Splunk, Cisco, and SentinelOne before joining Prowler as Head of Product.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: From Fuzzer Noise to a Weaponized PHP Exploit: Exploiting a PHP Use-After-Free Vulnerability

Tags: DEF CON Official Talk | Demo | Exploit

When: Sunday, Aug 9, 11:30 - 12:30 PDT

Where: LVCCW Level 1 Hall 3 906 (Main Track 3) - [Map](#)

Description:

It started as fuzzer noise: an OSS-Fuzz crash in PHP's `concat_function`, filed under a JIT target but with no JIT in the stack. It is a core Zend Engine use-after-free, reproducible with `php -n` and no extensions. This is an honest exploitability study on Linux x86-64: from the mistriaged crash to native command execution (arbitrary read/write via stale `DateInterval`, `zif_system` resolved in-process, ASLR and PIE defeated at runtime) even where `disable_functions` is set. It builds on the public exploitation lineage, with an SPL `ArrayObject` delivery trick as our own delta.

1. OSS-Fuzz Issue #483856591 — Original crash report filed under `php-fuzz-function-jit` target
2. PHP Source: `Zend/zend_operators.c`, `concat_function()` — https://github.com/php/php-src/blob/master/Zend/zend_operators.c
3. `php/php-src#16726` — Array-element UAF (second-chain vulnerability used to bypass mod-16 alignment barrier)
4. Zend MM Internals: https://www.phpinternalsbook.com/php7/memory_management/zend_memory_manager.html
5. CVE-2022-29072 — Prior 7-Zip zero-day by the same researcher (Kağan Çapar), demonstrating track record in vulnerability research
6. CVE-2026-5201 — `gdk-pixbuf` heap buffer overflow discovered by the same researcher, acknowledged by Red Hat (CVSS 7.5)
7. W3Techs PHP Usage Statistics — <https://w3techs.com/technologies/details/pl-php>
8. V8 Sandbox Design (2024) — Referenced in comparative interpreter memory model analysis

Speakers: Can Oztas, Kağan Çapar

SpeakerBio: Can Oztas

Can Oztas is a security researcher with applied R&D experience across several key sectors, including defense, finance, and telecommunications. His background encompasses AppSec, vulnerability research, and offensive security engineering. He is currently a PhD student focusing on the intersection of Artificial Intelligence and cybersecurity.

SpeakerBio: Kağan Çapar

Kağan Çapar is a Vulnerability Researcher with over 15 years of experience. His research focuses on binary exploitation, fuzzing, and zero-day discovery across widely deployed software.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Red Team Village - Friday - 10:00-17:59 PDT

Title: From Kiosk to Domain Compromise: Learning to Walk Up and Take it All

Tags: Red Team Village | Misc

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 309 (Red Team Village) Kiosk Area - [Map](#)

Description:

Kiosks are everywhere. Their prevalence in our society has exploded, with devices such as fast-food ordering, signage, ticketing and check-in, print/ship/office, library, point-of-sale, and more - all around us.

How secure are they though? Are they being adequately tested? We all learned on July 19, 2024, when a multitude of the signs and kiosks around us went BSOD that a large number of these kiosks – from airports to ATMs – are running on Windows. We need to be asking questions like, are they joined to a domain, what is network adjacent, and how could these systems lead to a serious attack path?

In this workshop we will walk through how to hack and secure kiosks in a four-part workshop, which will move from initial compromise to lateral movement and domain compromise, concluding with some defensive recommendations to prevent 'kiosk to domain takeover' scenarios.

Speakers: Ezra Woods, Mike Manrod, Spencer Alessi

SpeakerBio: Ezra Woods

Avid security researcher currently working as an Information Security Engineer with Grand Canyon Education

SpeakerBio: Mike Manrod

Mike, AKA, CroodSolutions, presently serves as CISO for Grand Canyon Education, teaches Malware Analysis for GCU, and helps lead the Threat Intelligence Support Unit.

In addition to work on BypassIT, AutoPwnKey, BYOEDR, and BeaconatorC2 with Ezra Woods and other contributors, Mike has served as a threat prevention engineer for Check Point along with various other roles.

He is also a co-author/contributor for the joint book project, Understanding New Security Threats published by Routledge in 2019, along with multiple articles/whitepapers. When not working, he spends time playing video games or working on cars with his kids.

SpeakerBio: Spencer Alessi

Spencer is a passionate security practitioner, with the heart of a defender and spirit of a hacker. Spencer's background is in IT and Systems Administration prior to making the transition to security. He leans on these crucial technical skills to help enable clients and security programs to build defensible, vigilant, and practical security programs. Most of Spencer's current efforts are focused on understanding threats, techniques, and methods and then implementing them through technical assessments and analysis. Spencer is Co-Host of The Cyber Threat Perspective podcast and regularly creates blogs, videos and other content. In November 2025 Spencer was awarded Microsoft MVP in Security - Identity & Access.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file



Title: From Live Malware to Red Team Tradecraft: Process Hollowing in msbuild.exe

Tags: La Villa Community | Creator Talk/Panel

When: Saturday, Aug 8, 15:30 - 16:30 PDT

Where: LVCCW Level 1 Hall 4 1416 (La Villa Community) Main Stage - [Map](#)

Description:

The best hiding place is often a binary Microsoft already signed. This talk presents a complete red team operation reconstructed from a real multi-stage JScript dropper captured in April 2026 targeting Energy, Government, and Aerospace organizations. Using custom tooling and malware analysis, we transformed the adversary's workflow into a repeatable offensive playbook focused on trusted binary abuse, fileless execution, and stealthy process injection.

The session demonstrates how attackers delivered a .NET payload through steganographic C2 hosted on trusted paste services, loaded assemblies directly in memory with `Reflection.Assembly::Load()`, and performed Process Hollowing into `msbuild.exe` using native Windows APIs including `ZwUnmapViewOfSection`, `VirtualAllocEx`, and `SetThreadContext`.

We also explore operational evasion techniques such as WMI hidden process spawning, obfuscated Base64 transformations, and Sysmon telemetry analysis from the perspective of a red team operator. Every technique shown was extracted from a live adversary sample and operationalized for realistic adversary emulation.

SpeakerBio: Filipi Pires, Head of Technical Advocacy at SCYTHE

I've been working as Head of Technical Advocacy at SCYTHE, Founder & Investor at CROSS-INTEL, Advisor & Investor at Sherlockeye, BSides Porto Organizer, Red Team Village Director (DEF CON), Senior Advisor Raices Cyber Academy, Founder of Red Team Community (Brazil and LATAM), AWS Community Builder, Snyk Ambassador, Application Security Specialist and Hacking is NOT a crime Advocate. International Speaker at Security and New technologies events in many countries such as US (Black Hat & Defcon), Canada, France, Spain, Germany, Poland, Black Hat MEA - Middle-East - and others, I've served as University Professor in Master Degree in Portugal, Graduation and MBA courses at Brazilian colleges, in addition, I'm Creator and Instructor of the Course - Malware Attack Types with Kill Chain Methodology (PentestMagazine), PowerShell and Windows for Red Teamers(PentestMagazine) and Malware Analysis - Fundamentals (HackerSec).

Black Hat US 2025 - <https://blackhat.com/us-25/arsenal/schedule/presenters.html#filipi-pires-46329> Black Hat US 2024 - <https://blackhat.com/us-24/arsenal/schedule/presenters.html#filipi-pires-46329> Black Hat MEA 2025 - <https://blackhatmea.com/speaker/filipi-pires-0> Black Hat MEA 2024 - <https://blackhatmea.com/speaker/filipi-pires> DEF CON 33 / 32 - <https://sessionize.com/filipi-pires/> DEF CON - Adversary Village - <https://adversaryvillage.org/adversary-events/DEFCON-33/Filipi-Pires/>



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Telecom Village - Saturday - 11:45-12:30 PDT

Title: From ONT to STB: Detecting IPTV Attack Chains in the Telecom SOC

Tags: Telecom Village | Creator Talk/Panel

When: Saturday, Aug 8, 11:45 - 12:30 PDT

Where: LVCCW Level 3 W321 (Telecom Village) - [Map](#)

Description:

1. IPTV Architecture – How IPTV is delivered over FTTH/GPON and the security implications of ONTs and STBs.
2. Weak Links – Common vulnerabilities in ISP-managed ONTs.
3. ONT to STB Attack Chain – A real-world red team attack demonstrating remote compromise and IPTV manipulation.
4. Telecom SOC Detection – Detecting ONT compromises through management, authentication, configuration, and IPTV traffic monitoring.

SpeakerBio: Zibran Sayyed

No BIO available

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Red Team Village - Saturday - 10:00-11:59 PDT

Title: From Path Traversal to Domain Credentials in 90 Seconds

Tags: Red Team Village | Misc

When: Saturday, Aug 8, 10:00 - 11:59 PDT

Where: LVCCW Level 1 Hall 1 309 (Red Team Village) Tactic Table 1 - [Map](#)

Description:

In this hands-on tactic, attendees will exploit a realistic document management portal to chain path traversal into something far more dangerous. We'll demonstrate a complete attack path from initial discovery to domain credentials, then discuss why this works, where you'll find it, and how defenders should be looking for it.

What You'll Do: You'll get hands-on access to a vulnerable Windows IIS application and work through the complete exploitation chain. By the end of the session, you'll have captured real domain credentials and understand exactly how the attack works at each step.

Basic familiarity with web vulnerabilities helpful but not required. We'll explain the concepts as we exploit them.

SpeakerBio: Mike Lisi

Mike helps organizations identify, prioritize, and eliminate real-world security risks before attackers exploit them. As Founder & CEO of Maltek Solutions, he brings over 15 years of hands-on experience across penetration testing, risk assessments, and cyber capability development. In addition to his consulting leadership, Mike serves as President of Red Team Village, a 501(c)(3) nonprofit delivering free offensive security training to a global community. Mike also leads CTF design for NCAE CyberGames, engaging 1,000+ collegiate participants annually.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: From Pipeline to Cloud Control

Tags: Cloud Village | Creator Talk/Panel

When: Friday, Aug 7, 11:30 - 12:10 PDT

Where: LVCCW Level 3 W313 (Cloud Village Talks) - [Map](#)

Description:

Azure DevOps service connections are a core part of modern pipelines, allowing teams to interact with Azure and other external systems seamlessly. While they make deployments faster and easier, they also introduce an attack surface that is often overlooked in real-world environments.

In this research, we explore new attack paths showing how even limited access within Azure DevOps pipelines can be leveraged to escalate privileges and compromise cloud environments. By taking advantage of over-scoped service connections and certain platform behaviors, an attacker can chain together small gaps to achieve significant impact, including gaining subscription-level access.

These findings were reported to Microsoft and acknowledged through MSRC, highlighting a deeper issue in how DevOps integrations are secured. Rather than being just a configuration problem, this reflects a broader gap that organizations need to understand when designing their cloud security approach.

SpeakerBio: Saksham Agrawal

Saksham Agrawal is a Senior Security Consultant at NotSoSecure, specializing in cloud security. His work focuses on discovering new attack paths in cloud environments and helping organizations understand real-world risks. He has presented his research at DEF CON Cloud Village, where he introduced his tool NoPrompt and shared practical techniques for cloud security testing. He enjoys building tools, exploring cloud internals, and sharing his findings with the security community. He has also responsibly reported critical vulnerabilities in major cloud vendors as part of his independent security research and actively delivers training sessions on cloud security and offensive security techniques.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: From Policy to Prod: How a Frontier AI Lab Enforces its Cyber Rules

Tags: Policy @ DEF CON | Creator Talk/Panel

When: Saturday, Aug 8, 11:00 - 11:59 PDT

Where: LVCCW Level 2 W210-211 (Policy Village) - [Map](#)

Description:

Every frontier AI lab publishes policies, but far less is known about what happens between a line in that policy and a blocked request in production. On Anthropic's safeguards team, we operate in that gap. In this talk, we'll walk through the full enforcement lifecycle at Anthropic: how policy gets written, how we translate it into evals that actually measure the behavior we care about, how we build precision-tuned classifiers to detect misuse traffic at scale, and how those classifiers feed a layered enforcement stack. We'll share what's worked, what hasn't, and the open problems we think the policy community should be paying attention to.

Speakers: Grant Versfeld, David "0xdf" Forsythe

SpeakerBio: Grant Versfeld, Anthropic

Grant Versfeld co-leads cyber enforcement on Anthropic's Safeguards team, where he bridges the Policy and Threat Intelligence teams to disrupt cyber threat actors. Before Anthropic, he was a security engineer for Google Cloud Threat Intelligence, investigating nation-state campaigns against Cloud customers, contributing to Google Cloud's Threat Horizons report, and supporting Mandiant's cyber espionage research. He is a former Cybersecurity Policy Fellow at the Center for Democracy & Technology, a Hackers on the Hill ambassador, and a judge for Atlantic Council's Cyber 9/12 competition. He returns to DEF CON having previously played the FBI agent in DC 31's Hacker Court.

SpeakerBio: David "0xdf" Forsythe, Anthropic

David Forsythe (0xdf) is a member of technical staff at Anthropic working on cybersecurity strategy and safeguards for frontier AI. Before that, 20+ years across the US public and private sectors in SOC/CIRT, threat intelligence, red teaming, threat research, and education, most recently as Principal Lab Architect at HackTheBox.

He is also a long-running security content creator, publishing CTF walkthroughs and technical breakdowns of exploits and other security topics at 0xdf.gitlab.io and on YouTube. As a player, he has reached as high as 4th on the HackTheBox global leaderboard, is a two-time Best Overall winner of the SANS Holiday Hack Challenge, and a three-time SANS NetWars Tournament of Champions team winner.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Blacks In Cyber Village - Sunday - 10:00-10:59 PDT

Title: From Practitioner to Principal: Building a Cybersecurity Business That Lasts

Tags: Blacks In Cyber Village | Creator Workshop

When: Sunday, Aug 9, 10:00 - 10:59 PDT

Where: LVCCW Level 3 W322-W324 (BIC Village) - [Map](#)

Description:

Most cybersecurity workshops teach you how to do the work. This one teaches you how to own it. Tyrone E. Wilson Army veteran, CISO, and founder of Cover6 Solutions breaks down what it actually takes to transition from practitioner to principal: building a service-based firm, pricing your expertise, navigating GovCon as an SDVOSB, and sustaining a business that doesn't depend on your last client check.

SpeakerBio: Tyrone E. Wilson, Cover6 Solutions

Tyrone E. Wilson is a U.S. Army veteran, cybersecurity executive, and founder of Cover6 Solutions a Service-Disabled Veteran-Owned Small Business delivering vCISO and compliance services to organizations across the public and private sectors. With over two decades of experience in security leadership, they built Cover6 from the ground up while simultaneously growing a 9,000+ member cybersecurity community for career changers and professionals of color. They are the creator of the Breaking Into Cyber framework and host of the Cover6 Community a free resource for anyone navigating the industry without a built-in network. Tyrone has delivered training for Blacks In Cybersecurity and speaks regularly on the intersection of entrepreneurship, community, and cybersecurity career development.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: From Prompts to Production: Discovering Exposed PII & IDORs in AI-Generated Apps

Tags: Intermediate | AppSec Village | Creator Talk/Panel

When: Saturday, Aug 8, 17:30 - 17:59 PDT

Where: LVCCW Level 1 Hall 2 604 (Appsec Village) Main Stage - [Map](#)

Description:

Users building apps with vibe coding platforms like Lovable or Base44 often overlook critical security vulnerabilities. As these platforms gain rapid adoption, thousands of apps are being created without sufficient attention to security, leaving significant flaws in plain sight. Our research, conducted across thousands of apps, revealed widespread issues, including 175 instances of sensitive PII leakage (such as medical records and personal contact information), SSRF, 0-click account takeovers, and IDORs.

In this talk, we'll share our field experience in developing discovery and security testing techniques that uncover exploitable web app and API behaviors at scale. We'll walk through concrete examples, showing how critical vulnerabilities hide in plain sight and how even minor misconfigurations can lead to catastrophic breaches. Attendees will learn to identify these security risks and secure their no-code apps, including best practices for handling sensitive data and securing APIs.

SpeakerBio: Samantha Pearlstein, Founding Solutions Engineer at Escape

Samantha is a solutions engineer with a strong background in security research, executive cyber resilience, and nation-state threats. As a former consultant at Accenture, she led cyber resilience initiatives for Fortune 100 executives, developed GenAI-powered security tools, and delivered workshops on emerging cyber challenges. Today, as a Sales Engineer at Escape, Samantha helps AppSec teams secure their APIs and SPAs, combining her passion for cybersecurity with hands-on problem-solving.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: From Roots to Renaissance: The Rising Generation of Middle Eastern and African Cybersecurity

Tags: Middle Easterns & Africans in Cyber Security (MEACS) | Creator Talk/Panel

When: Sunday, Aug 9, 10:00 - 10:59 PDT

Where: LVCCW Level 1 Hall 4 1306 (Middle Easterns & Africans in Cyber Security (MEACS) Community) - [Map](#)

Description:

If yesterday was where we came from, today is where we are going. The same regions that gave the world algebra and the first codebreakers are now home to some of the fastest-growing security communities on the planet, from Lagos to Cairo to Riyadh, alongside a diaspora shaping the field from inside every major company and conference. This talk picks up where the kickoff left off and moves from history to right now: the researchers, founders, defenders, and organizers carrying the work forward, the obstacles that still stand in the way, and what it takes to build a career and a community when the industry has not always made room for you. We will talk honestly about representation, mentorship, and momentum, and about the role a space like MEACS plays in turning a shared heritage into a shared future. Come for the story, stay to find your people.

SpeakerBio: Ezz Tahoun

Ezz Tahoun is an award-winning cybersecurity data scientist recognized globally for his innovations in applying AI to security operations.

He has keynoted, trained & presented at BlackHat US, Sector, MEA, Asia & EU, DEFCON, SANS Summits, all the top Bsides, Securityweek ICS Conference and GISEC among many others.

His groundbreaking work earned him a gold edison award and accolades from Yale, Princeton, Northwestern, NATO, Microsoft, and Canada's CSE.

At 19, Ezz began his PhD in Computer Sci at the Univ of Waterloo, quickly gaining recognition through over 20 influential papers and open-source tools.

His experience includes leading advanced AI security ops projects for Orange CyberDefense, Forescout, RBC, and Huawei US.

He holds certifications such as GIAC Advisory Board, aCCISO, CISM, CRISC, GCIH, CEH, PMP and GCP-Cloud Architect, and served as an adjunct professor in cyber defense and warfare.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: From square root to /root: escalating privileges in Azure containers with Python in Excel

Tags: DEF CON Official Talk | Demo | Tool | Exploit

When: Friday, Aug 7, 10:00 - 10:59 PDT

Where: LVCCW Level 1 Hall 3 903 (Main Track 5) - [Map](#)

Description:

Microsoft integrated Python into Excel, giving users more advanced data analysis. The Python code is processed in a cloud container and returned as results. This sparks an immediate question: does it allow remote code execution on Microsoft owned servers?

In this talk, we'll dig into the various web applications and components in the Python execution environment. We'll describe how we discovered a privilege escalation vulnerability in the file upload mechanism of this service, which allowed us to gain root access within the container. Utilizing that, we revealed the complete architecture of this solution. We will show how we discovered Microsoft's internal deployment configuration, including key vaults, database servers, account names, tenant IDs, and much more. We were even able to execute code on the pilot servers of this product.

We also found how to craft a special response to Excel, resulting in bypassing two security boundaries (CVE-2026-45459): the trusted records protection ("Enable Content" warning) and the network isolation protection.

We will expose features that weren't even announced yet and how they might be exploited. Follow us in our journey from the first "whoami" command, through exfiltrating tailor-made Python libraries, and eventually finding a vulnerability to achieve execution as root!

<https://i.blackhat.com/Asia-25/Asia-25-Carmel-The-Problems-of-Embedded-Python-in-Excel.pdf>

<https://www.netspi.com/blog/technical-blog/red-teaming/a-first-look-at-python-in-excel/>

SpeakerBio: Ron Ben Yizhak, SafeBreach

Ron (@RonB_Y) is a security researcher at SafeBreach with 11 years of experience. He works in vulnerability research and has knowledge in forensic investigations, malware analysis and reverse engineering. Ron previously worked in the development of security products and spoke several times at DEF CON

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Adversary Village - Friday - 13:15-13:59 PDT

Title: From threat-intel to tested defense, the adversary simulation playbook

Tags: Adversary Village | Creator Talk/Panel

When: Friday, Aug 7, 13:15 - 13:59 PDT

Where: LVCCW Level 1 Hall 3 1105 (Creator Stage 3) - [Map](#)

Description:

Knowing who is coming for you is only half the fight. The real work is turning that knowledge into defenses that actually works. This panel walks through the full playbook, from raw threat intelligence on state-sponsored actors and other adversaries, to emulating their tradecraft, to validating whether your defenses can really stand up to it. Our panelists bring hands-on experience across adversary simulation, threat intel, and purple teaming to talk about what it takes to move from a report on paper to a tested, measurable defensive posture. The panel will dig into how to prioritize the threats that matter to your organization, how to faithfully replicate real adversary behavior instead of chasing generic checklists, and how red and blue working side by side turns every simulated attack into a lasting defensive victory. Whether you are defending against nation-state operators or opportunistic criminals, the goal is the same! Stop guessing about your defenses and start proving them. Join us for a practical conversation about closing the gap between intelligence and action.

Speakers: Cheryl Biswas, Adam Pennington, Olaf Hartong, Sarah Hume

SpeakerBio: Cheryl Biswas, Strategic Threat Intel Analyst at TD Bank

Cheryl Biswas is a Strategic Threat Intel Analyst with TD bank in Toronto, Canada. She found her way into InfoSec through a helpdesk backdoor and pivoted into roles for vendor and change management, jumped a gap into privacy and DR/BCP, then laterally moved into security audits and assessments. Her degree in Political Science has evolved into researching APTs, botnets, ransomware and more. Cheryl is actively involved in the security community as a conference speaker and volunteer, mentors those entering the field, and encourages women and diversity in Infosec as a founding member of the "The Diana Initiative."

SpeakerBio: Adam Pennington, ATT&CK lead at MITRE Corporation

Adam Pennington leads ATT&CK at The MITRE Corporation and collected much of the intelligence leveraged in creating ATT&CK's initial techniques. He has spent much of his 16 years with MITRE studying and preaching the use of deception for intelligence gathering. Prior to joining MITRE, Adam was a researcher at Carnegie Mellon's Parallel Data Lab and earned his BS and MS degrees in Computer Science and Electrical and Computer Engineering from Carnegie Mellon University. Adam has presented and published in several venues including FIRST CTI, USENIX Security, DEF CON, and ACM Transactions on Information and System Security.

SpeakerBio: Olaf Hartong, Defensive Specialist at FalconForce

Olaf Hartong is a Defensive Specialist and security researcher at FalconForce. He specialises in understanding the attacker tradecraft and thereby improving detection. He has a varied background in blue and purple team operations, network engineering, and security transformation projects. Olaf has presented at many industry conferences including Black Hat, DEF CON, DerbyCon, Splunk .conf, FIRST, MITRE ATT&CKcon, and various other conferences. Olaf is the author of various tools including ThreatHunting for Splunk, ATTACKdatamap and Sysmon-modular. He maintains a blog at <https://olafhartong.nl>

SpeakerBio: Sarah Hume, Purple Team Service Lead at Security Risk Advisors

Sarah leads the Purple Team service at Security Risk Advisors (SRA). She has led hundreds of Threat Intelligence-based Purple Team exercises for organizations in the Fortune 500 and Global 1000 over the past 7 years. Her background is in

offensive security, primarily internal network, OT/ICS, and physical security penetration testing. Sarah also has experience in external network penetration testing, web application assessments, OSINT, phishing/vishing campaigns, vulnerability management, and cloud assessments. Sarah graduated Summa Cum Laude from Penn State with a B.S. in Cybersecurity. She is a Certified Red Team Operator (CRTO), Certified Information Systems Security Professional (CISSP), Google Digital Cloud Leader, AWS Certified Cloud Practitioner, and Advanced Infrastructure Hacking Certified. She lives in Philadelphia with her dog, Paxton.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: From Wind Farm to CHP Plant: The Untold Story of Lateral Movement in a Polish Energy Sector Attack

Tags: DEF CON Official Talk

When: Saturday, Aug 8, 10:00 - 10:59 PDT

Where: LVCCW Level 1 Hall 3 903 (Main Track 5) - [Map](#)

Description:

On December 29, 2025, Poland's energy sector was hit by what we believe was the first destructive cyber sabotage attack against energy infrastructure in NATO. Our public report described attacks against 30 renewable energy sites and a large combined heat and power plant. But one piece of the incident was still missing - and it led to an attack path we had never seen in the wild before.

This talk goes behind the scenes of the investigation into a second, smaller CHP plant affected during the same campaign. What first looked like human error turned into a three-month hunt through false leads, forgotten remote access devices, wiped industrial hardware, cellular connectivity, and infrastructure that was assumed to be isolated.

The talk ends with lessons on private APN security, OT incident response, and handling large-scale cyber incidents involving critical infrastructure.

SpeakerBio: Marcin Dudek, CERT.PL

Marcin Dudek leads CERT Polska, Poland's national CERT. Before taking on this role, he spent more than a decade in hands-on technical work across OT security, incident response, and APT investigations. His background includes industrial control systems security in critical infrastructure environments, including Poland's only research nuclear reactor, as well as analysis of APT activity targeting Poland. He regularly speaks at local and international cybersecurity conferences and was deeply involved in the response to the incident described in this talk.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Telecom Village - Saturday - 14:15-14:45 PDT

Title: From Zero-Day to Zero-Hour: Rethinking Telecom Defense for the Frontier AI Era

Tags: Telecom Village | Creator Talk/Panel

When: Saturday, Aug 8, 14:15 - 14:45 PDT

Where: LVCCW Level 3 W321 (Telecom Village) - [Map](#)

Description:

Details:

Frontier AI is changing the economics and speed of cyberattacks—compressing vulnerability discovery, exploitation, and attack automation from days to potentially hours or minutes. For telecom networks and their complex OEM and supply-chain ecosystem, traditional vulnerability management and defense models may no longer be fast enough.

This session explores how telecom operators, OEMs, security teams, and regulators must adapt for the frontier AI era—from AI-driven vulnerability discovery and autonomous attacks to faster remediation, AI-powered defense, supply-chain resilience, and coordinated industry response. The key question: when attackers operate at machine speed, can telecom defense keep up?

SpeakerBio: Arvind Singh

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: from_pretrained() to from_pwned(): Breaking HuggingFace's Trust

Tags: Intermediate | AppSec Village | Creator Talk/Panel

When: Friday, Aug 7, 14:10 - 14:40 PDT

Where: LVCCW Level 1 Hall 2 604 (Appsec Village) Main Stage - [Map](#)

Description:

uggingFace has become the GitHub of machine learning. Two million models, 15 million daily downloads. We discovered a critical RCE (CVE-2026-4372) that compromises any machine loading a malicious model. Add one field to a model's config.json, publish it on the Hub, and any standard from_pretrained() call is silently compromised. No trust_remote_code=True. No warnings. The one security boundary the entire ML ecosystem relies on, bypassed completely.

The chain is three flaws: a generic setattr loop stamping every JSON field onto the config object including private attributes; a sanitization gap protecting the public interface but not the underscore-prefixed internal equivalent; and an unsandboxed kernel loader executing arbitrary Python from any Hub repo. One field weaponizes all three.

We walk through the full attack chain live. Model registries are the new package registries, facing the same supply-chain threats that broke the software world - with far less mature defenses.

SpeakerBio: Yotam Perkal

Yotam Perkal leads security research at Pluto Security, a next-generation AI security and governance platform designed to protect the rapidly emerging ecosystem of AI builders, low-code/no-code tools, and agentic applications. His work focuses on securing AI-native development environments and building scalable methods for detecting, validating, and mitigating risks in AI-driven software workflows.

Previously, Yotam led the Threat Research team at Zscaler, headed the Vulnerability Research team at Rezilion, and held multiple roles within PayPal's security organization across vulnerability management, threat intelligence, and insider threat.

Yotam is an active participant in several cross-industry working groups dealing with AI security, vulnerability management, and supply chain security.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Social Gatherings/Events - Saturday - 21:00-00:59 PDT

Title: Front Man's Fête: An Octopus Game Party (including Octopus Game winners and prizes)

Tags: Party | Octopus Game

When: Saturday, Aug 8, 21:00 - 00:59 PDT

Where: LVCCW Level 2 W212 (Misc Meeting Room) - [Map](#)

Description:

Front Man's Fête: An Octopus Game Party is a curated respite from the chaos of the city, offering a sophisticated and low-key lounge experience centered on strategy and soul. Instead of high-stakes elimination, we offer the timeless rhythm of old school hip-hop and the analog competition of classic board games. This event is designed for those who seek a chill atmosphere where the vibes are smooth and the conversation is clear. Come for the nostalgia of golden-era beats and stay for a relaxed evening where the only goal is to unwind and outsmart your opponents in a sanctuary of cool.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: FTS Build it Yourself: cDc X OWASP X Veilid

Tags: OWASP Foundation | Creator Talk/Panel

When: Saturday, Aug 8, 13:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 4 1415 (OWASP Foundation) - [Map](#)

Description:

Join us for a state of Veilid update, where we'll explore the latest progress, milestones, and what's next for the project as it continues to build a decentralized, privacy-first communications and networking platform.

After the presentation, stick around for an open discussion about what it really takes to escape today's digital walled gardens. We'll talk about the challenges of reducing dependence on centralized services, the practical realities of building and adopting self-hosted and decentralized alternatives, and how open source communities can create tools that preserve privacy, autonomy, and user ownership.

Speakers:Gibson,medus4,cdC & Veilid crew

SpeakerBio: Gibson

No BIO available

SpeakerBio: medus4

No BIO available

SpeakerBio: cdC & Veilid crew

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Bug Bounty Village - Sunday - 11:00-11:30 PDT

Title: Full Disclosure, Full Screen: [Informative] The Story of Bug Bounty Village Badge 2026

Tags: Bug Bounty Village | Creator Talk/Panel

When: Sunday, Aug 9, 11:00 - 11:30 PDT

Where: LVCCW Level 2 W206-207 (Bug Bounty Village) - [Map](#)

Description:

Every year the BBV badge gets one new thing we don't know how to do yet. Last year: epoxy. This year: a real 0.96" OLED behind the acrylic, giving a whole new vibe to the hacker laptop screen. Plus RGB for whichever team you're on, and a fun CTF.

SpeakerBio: Abhinav "TweetsFromPanda" Pandagale, Founder, Hackerware

Abhinav's artistry comes from the times he used to sneakily paint drawings made by his sister. His hacking career began as a toddler, disassembling his toys but never putting them back together. His entrepreneurial roots come from selling snacks at a school fair and making a loss of ten bucks, his entire pocket money. Having learned how not to make money, he launched Hackerware.io - a boutique badgelifelab with in-house manufacturing - which has grown over the past ten years into a global presence across 20+ countries. He's often spotted at conferences around the world - hosting hardware villages or pulling off the kind of random shenanigans that earned him the Sin CON Person of the Year 2025 award.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

DEF CON Training - Saturday - 08:30-17:30 PDT

Title: Full-Stack Pentesting Laboratory: 100% Hands-On + Lifetime LAB Access

Tags: DEF CON Training (Paid) (2-day) | DEF CON Training

When: Saturday, Aug 8, 08:30 - 17:30 PDT

Where: LVCCW Level 2 W224 (Training) - [Map](#)

Description:

SpeakerBio: Dawid Czagan

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

DEF CON Training - Sunday - 08:30-17:30 PDT

Title: Full-Stack Pentesting Laboratory: 100% Hands-On + Lifetime LAB Access

Tags: DEF CON Training (Paid) (2-day) | DEF CON Training

When: Sunday, Aug 9, 08:30 - 17:30 PDT

Where: LVCCW Level 2 W224 (Training) - [Map](#)

Description:

SpeakerBio: Dawid Czagan

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Hackers.town - Saturday - 14:00-14:59 PDT

Title: Fun with alternative smartphones with The Tech Reclaimers!

Tags: Hackers.town | Creator Talk/Panel

When: Saturday, Aug 8, 14:00 - 14:59 PDT

Where: LVCCW Level 1 Hall 4 1420 (Hackers.town) - [Map](#)

Description:

SpeakerBio: Janet Vertesi, Officer at Tech Reclaimers

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Queercon Community - Friday - 15:00-15:59 PDT

Title: Furs and Kinksters Meetup

Tags: Queercon Community | Creator Event/Activity

When: Friday, Aug 7, 15:00 - 15:59 PDT

Where: LVCCW Level 3 W325 (QueerCon Lounge) - [Map](#)

Description:



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Contests - Sunday - 10:00-10:30 PDT

Title: Game Hacking Village CTF awards ceremony

Tags: Game Hacking Village | Game Hacking Village CTF | Contest

When: Sunday, Aug 9, 10:00 - 10:30 PDT

Where: LVCCW Level 1 Hall 1 211 (Game Hacking Village) - [Map](#)

Description:

Winners of the Game Hacking Village CTF will be awarded their prizes.



[Return to Index](#) - Add to Google

- ics [Calendar](#) file

Contests - Sunday - 10:00-11:59 PDT

Title: Game Hacking Village CTF Q&A / Walkthroughs

Tags: Game Hacking Village | Game Hacking Village CTF | Contest

When: Sunday, Aug 9, 10:00 - 11:59 PDT

Where: LVCCW Level 1 Hall 1 211 (Game Hacking Village) - [Map](#)

Description:

A presentation by the challenge creators about how the Game Hacking Village CTF along with an open QnA about challenges.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Contests - Saturday - 10:00-17:59 PDT

Title: Game Hacking Village CTF

Tags: Game Hacking Village | Game Hacking Village CTF | Contest

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 211 (Game Hacking Village) - [Map](#)

Description:

Compete against other teams to be the first to hack all of our games on our custom Mist Store platform



[Return to Index](#) - Add to Google

- ics [Calendar](#) file

Contests - Friday - 10:00-17:59 PDT

Title: Game Hacking Village CTF

Tags: Game Hacking Village | Game Hacking Village CTF | Contest

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 211 (Game Hacking Village) - [Map](#)

Description:

Compete against other teams to be the first to hack all of our games on our custom Mist Store platform

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Game Hacking Village - Saturday - 12:00-12:59 PDT

Title: Game Hacking with AI

Tags: Game Hacking Village | Creator Talk/Panel

When: Saturday, Aug 8, 12:00 - 12:59 PDT

Where: LVCCW Level 1 Hall 1 211 (Game Hacking Village) - [Map](#)

Description:

This informal talk is intended to cover expert usage of AI agents using Claude/Codex and how you can apply them to be effective in areas like game hacking. How do you keep an agent on track, how do you make it more accurate, more efficient, and how do you get it to go around guiderails. If you're using AI in a web browser or copy+pasting code (in game hacking or otherwise) this talk is for you.

SpeakerBio: Juno, Game Hacking Village

No BIO available

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

CodeBloom - Saturday - 15:00-15:59 PDT

Title: Game Time: Input, Output, and Variables

Tags: CodeBloom | Creator Workshop

When: Saturday, Aug 8, 15:00 - 15:59 PDT

Where: LVCCW Level 1 Hall 4 1304 (CodeBloom Community) - [Map](#)

Description:

Input, output, and variables are the building blocks behind every single program you've ever used, and once you understand them, you're well on your way to writing your own code! In this session, we'll play some fun games together to show how these ideas already show up in your everyday life, then practice matching them to real Python code. All are welcome, no coding experience required. If you've ever wanted to get involved in our community or teach our classes, this would be a great time to stop by and learn more!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

CodeBloom - Friday - 15:00-15:59 PDT

Title: Game Time: Input, Output, and Variables

Tags: CodeBloom | Creator Workshop

When: Friday, Aug 7, 15:00 - 15:59 PDT

Where: LVCCW Level 1 Hall 4 1304 (CodeBloom Community) - [Map](#)

Description:

Input, output, and variables are the building blocks behind every single program you've ever used, and once you understand them, you're well on your way to writing your own code! In this session, we'll play some fun games together to show how these ideas already show up in your everyday life, then practice matching them to real Python code. All are welcome, no coding experience required. If you've ever wanted to get involved in our community or teach our classes, this would be a great time to stop by and learn more!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Game Time: Input, Output, and Variables

Tags: CodeBloom | Creator Workshop

When: Sunday, Aug 9, 12:00 - 12:59 PDT

Where: LVCCW Level 1 Hall 4 1304 (CodeBloom Community) - [Map](#)

Description:

Input, output, and variables are the building blocks behind every single program you've ever used, and once you understand them, you're well on your way to writing your own code! In this session, we'll play some fun games together to show how these ideas already show up in your everyday life, then practice matching them to real Python code. All are welcome, no coding experience required. If you've ever wanted to get involved in our community or teach our classes, this would be a great time to stop by and learn more!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

CodeBloom - Saturday - 12:00-12:59 PDT

Title: Game Time: Input, Output, and Variables

Tags: CodeBloom | Creator Workshop

When: Saturday, Aug 8, 12:00 - 12:59 PDT

Where: LVCCW Level 1 Hall 4 1304 (CodeBloom Community) - [Map](#)

Description:

Input, output, and variables are the building blocks behind every single program you've ever used, and once you understand them, you're well on your way to writing your own code! In this session, we'll play some fun games together to show how these ideas already show up in your everyday life, then practice matching them to real Python code. All are welcome, no coding experience required. If you've ever wanted to get involved in our community or teach our classes, this would be a great time to stop by and learn more!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Game Time: Input, Output, and Variables

Tags: CodeBloom | Creator Workshop

When: Friday, Aug 7, 12:00 - 12:59 PDT

Where: LVCCW Level 1 Hall 4 1304 (CodeBloom Community) - [Map](#)

Description:

Input, output, and variables are the building blocks behind every single program you've ever used, and once you understand them, you're well on your way to writing your own code! In this session, we'll play some fun games together to show how these ideas already show up in your everyday life, then practice matching them to real Python code. All are welcome, no coding experience required. If you've ever wanted to get involved in our community or teach our classes, this would be a great time to stop by and learn more!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Game Time: Loops

Tags: CodeBloom | Creator Workshop

When: Sunday, Aug 9, 10:00 - 10:59 PDT

Where: LVCCW Level 1 Hall 4 1304 (CodeBloom Community) - [Map](#)

Description:

Have you ever had to do the same thing over and over and thought, there has to be an easier way? Good news, there is, and it's called a loop! Come play some classic schoolyard games with us and discover that you've been using loops in real life all along. Then we'll show you how programmers use for loops and while loops to make computers repeat tasks automatically, whether that's counting to 100 or spawning enemies in your favorite video game. No experience needed, just come ready to play! If you've ever wanted to get involved in our community or teach our classes, this would be a great time to stop by and learn more!

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Game Time: Loops

Tags: CodeBloom | Creator Workshop

When: Friday, Aug 7, 10:00 - 10:59 PDT

Where: LVCCW Level 1 Hall 4 1304 (CodeBloom Community) - [Map](#)

Description:

Have you ever had to do the same thing over and over and thought, there has to be an easier way? Good news, there is, and it's called a loop! Come play some classic schoolyard games with us and discover that you've been using loops in real life all along. Then we'll show you how programmers use for loops and while loops to make computers repeat tasks automatically, whether that's counting to 100 or spawning enemies in your favorite video game. No experience needed, just come ready to play! If you've ever wanted to get involved in our community or teach our classes, this would be a great time to stop by and learn more!

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Game Time: Loops

Tags: CodeBloom | Creator Workshop

When: Saturday, Aug 8, 10:00 - 10:59 PDT

Where: LVCCW Level 1 Hall 4 1304 (CodeBloom Community) - [Map](#)

Description:

Have you ever had to do the same thing over and over and thought, there has to be an easier way? Good news, there is, and it's called a loop! Come play some classic schoolyard games with us and discover that you've been using loops in real life all along. Then we'll show you how programmers use for loops and while loops to make computers repeat tasks automatically, whether that's counting to 100 or spawning enemies in your favorite video game. No experience needed, just come ready to play! If you've ever wanted to get involved in our community or teach our classes, this would be a great time to stop by and learn more!

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

The Diana Initiative - Saturday - 11:40-11:50 PDT

Title: Gamer Village Tour

Tags: The Diana Initiative | Creator Tour

When: Saturday, Aug 8, 11:40 - 11:50 PDT

Where: LVCCW Level 1 South Lobby / Atrium - [Map](#)

Description:

Interested in visiting Gamer Village but afraid to go by yourself? The Diana Initiative is hosting tours! Follow a volunteer to Gamer Village and be introduced to the community and activities inside!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Noob Community - Saturday - 11:45-12:45 PDT

Title: Gamifying the Matrix: a MITRE ATT&CK Video Game

Tags: Noob Community | Creator Talk/Panel

When: Saturday, Aug 8, 11:45 - 12:45 PDT

Where: LVCCW Level 1 Hall 4 1417 (Noob Community) - [Map](#)

Description:

This session introduces attendees to the MITRE ATT&CK Defense Game, a technical capstone project designed to bridge high-level gaming logic with real-world cybersecurity infrastructure. We will explore how gamification can be used to visualize adversary tactics and techniques in a controlled, interactive environment. The presentation covers the development of frontend interfaces and backend logic used to simulate defensive responses to various attack vectors, making complex security frameworks accessible to those just starting their journey in the field.

Speakers: Annie Meaney, Anne Drago

SpeakerBio: Annie Meaney

No BIO available

SpeakerBio: Anne Drago

No BIO available

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Recon Village - Friday - 11:00-16:59 PDT

Title: GE(O)SINT Contest

Tags: Recon Village | Creator Event/Activity

When: Friday, Aug 7, 11:00 - 16:59 PDT

Where: LVCCW Level 1 Hall 2 501 (Recon Village) - [Map](#)

Description:

Test your geospatial intelligence skills in this unique contest. Identify locations, analyze imagery, and demonstrate your GeoINT expertise.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Recon Village - Saturday - 11:00-16:59 PDT

Title: GE(O)SINT Contest

Tags: Recon Village | Creator Event/Activity

When: Saturday, Aug 8, 11:00 - 16:59 PDT

Where: LVCCW Level 1 Hall 2 501 (Recon Village) - [Map](#)

Description:

Test your geospatial intelligence skills in this unique contest. Identify locations, analyze imagery, and demonstrate your GeoINT expertise.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: GeoHacking: from memory corruption RCE to cross tenant access

Tags: Intermediate | AppSec Village | Creator Talk/Panel

When: Friday, Aug 7, 14:50 - 15:20 PDT

Where: LVCCW Level 1 Hall 2 604 (Appsec Village) Main Stage - [Map](#)

Description:

The tale of CVE-2026-40412, hacking Microsoft Planetary Computer Pro service. This talk will walk you through the journey of discovering a chain of vulnerabilities in the service itself and in its open source dependencies. All those findings combined resulted in cross tenant access. From a file read, to exploiting a buffer overflow (bypassing ASLR) to finding and exploiting a devastating design flaw. This talk will address the unique challenges of exploiting memory corruption bugs in cloud services, the pitfalls of cloud services' architecture and how we helped the engineering team fix the issues we found at the design level.

SpeakerBio: Michal Kamensky

Michal is a security researcher on the Microsoft STORM team, where she focuses on vulnerability research across the hybrid cloud domain. Previously she has worked as a security researcher at Bounce Security, and for the last few years volunteers as a Defcon goon. She enjoys diving into large code bases, understanding complex architectures, and eliminating vulnerabilities at scale.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Geolocating Talent: How OSINT CTFs are Building Tomorrow's Analysts

Tags: OSINT For Good Community | Creator Talk/Panel

When: Friday, Aug 7, 12:30 - 13:15 PDT

Where: LVCCW Level 1 Hall 4 1307 (OSINT4Good Community) Stage - [Map](#)

Description:

What happens when you hand students a daily "Cyber Briefing," a target, and unrestricted internet access? You build relentless investigators. In this talk, former Oracle vulnerability analyst turned educator Ben Crenshaw breaks down how to weaponize curiosity by scaling OSINT training from a single classroom to massive regional competitions. Drawing on his experience training 1000+ competitors for the Mayors Cyber Cup and coaching TraceLabs SearchParty CTFs, Ben will share exactly how to teach the threat-intel mindset. Discover how gamified open-source intelligence is reshaping cybersecurity education, turning passive scrollers into privacy-aware analysts, and building the next generation of defenders.

SpeakerBio: Ben "The Cyber Sensei" Crenshaw, Transofotech Academy | Cyber & AI Education Leader | EdTech & Workforce Development | U.S. Cyber Games Mentor | NICE Cybersecurity Ambassador | CLEAR AI Initiative | Senior TraceLabs Coach | Aerospace Education Member

Ben Crenshaw, known as The Cyber Sensei, is a cybersecurity educator, author of two industry books, and a dedicated US Cyber Games Mentor. Leveraging his background as a former Senior Vulnerability Analyst at Oracle, Ben transitioned into education to bridge the critical gap between real-world threat intelligence and classroom theory. Currently serving as Lead Cybersecurity instructor for Transfortech and as former Head of Cyber and AI Education at Work ED, he has taught Open-Source Intelligence (OSINT) to thousands of students, shaping them into ethically grounded, privacy-conscious defenders. A passionate advocate for scaling cyber education, Ben actively trains educators and coaches to prepare the next generation of talent for large-scale competitions like the Mayors Cyber Cup and TraceLabs.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Get Set, Exploit! Unveiling Python Class Pollution In-the-Wild

Tags: DEF CON Official Talk | Demo | Tool | Exploit

When: Saturday, Aug 8, 15:00 - 15:59 PDT

Where: LVCCW Level 1 Hall 3 906 (Main Track 3) - [Map](#)

Description:

Python is widely used in LLM applications and agent frameworks. Its ease of use comes from two core features: a uniform object model and dynamic reflection, which unfortunately also enable an emerging vulnerability class: Python class pollution. To date, with only one CVE and a handful of synthetic examples since its first disclosure in 2023, what is known is merely the tip of the iceberg, the real threat runs far deeper into the Python ecosystem.

In this talk, we introduce the first complete taxonomy of this vulnerability class, built from two object-resolution primitives and three object-assignment primitives, which together yield six types. Only one was previously known.

Building on this taxonomy, we design and implement Pyrl, the first automated framework for detecting Python class pollution via a novel static analysis technique named operational taint analysis. Applying Pyrl to over 600,000 GitHub and PyPI packages, we found 47 exploitable zero-days in Azure CLI, Taipy, ComfyUI, Google Mesop, HuggingFace Smolagents, and others. Through live case studies, we show how class pollution can be weaponized into token exfiltration, authentication bypass, stored XSS, sandbox escape, and RCE. Most importantly, we demonstrate that even the weakest type—one previously unknown—can still lead to critical impact in practice.

Speakers: Gavin Zhong, Zhengyu Liu, Jianjia Yu

SpeakerBio: Gavin Zhong, Johns Hopkins University

Jiacheng (Gavin) Zhong is a security researcher, focusing on AI system security, program analysis, and identity security. He recently completed his M.S. in Security Informatics at Johns Hopkins University, where his work was accepted to IEEE S&P 2026. Gavin has reported over 30 CVEs in widely used open-source projects. He is also an active CTF player with r3kapig, an international team ranked top 3 worldwide.

SpeakerBio: Zhengyu Liu, Johns Hopkins University

Zhengyu Liu is a third-year PhD student in Computer Science at Johns Hopkins University. His research focuses on web and software security via program analysis. His work received Distinguished Paper (S&P '25), Honorable Mention (USENIX '25), and Best Student Paper (ICICS '22). He is a DEF CON speaker and is a member of CTF team TheHackersCrew.

SpeakerBio: Jianjia Yu, Johns Hopkins University

Jianjia Yu is a PhD student at Johns Hopkins University, advised by Prof. Yinzhao Cao. Her research focuses on security and privacy in web and mobile ecosystems using program analysis techniques. Her work has received Distinguished Paper Awards at CCS '23 and S&P '25, and an Honorable Mention at USENIX Security '25. She has discovered over 40 zero-day vulnerabilities and uncovered privacy leaks affecting millions of users across browser extensions and mobile applications.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Getting Started in OT/ICS Cybersecurity

Tags: Noob Community | Creator Talk/Panel

When: Saturday, Aug 8, 13:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 4 1417 (Noob Community) - [Map](#)

Description:

Industrial Control Systems (ICS) and Operational Technology (OT) run the world around us. Power plants, offshore oil rigs, trains, and other transportation systems, manufacturing plants – these are just a few examples of the critical infrastructure that society depends on. Each ICS/OT environment is unique and has specialized security requirements.

Protecting critical infrastructure becomes increasingly important each day as the frequency of cyberattacks and the number of attackers continue to grow. State adversaries are no longer the only ones targeting these specialized environments. Today's attackers include ransomware groups, hackers, cyber mercenaries, and more.

ICS/OT cybersecurity can seem complicated and even daunting at first, but it does not have to be. This session will help participants understand the fundamentals of how these environments operate and how to secure them with a practical, simple approach.

SpeakerBio: Mike Holcomb

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Ham Radio Village - Friday - 12:00-12:30 PDT

Title: Getting Started In Radio Direction Finding

Tags: Ham Radio Village | Creator Talk/Panel

When: Friday, Aug 7, 12:00 - 12:30 PDT

Where: LVCCW Level 3 W315 (Ham Radio Village) - [Map](#)

Description:

Radio Direction Finding (RDF) is one of the most practical and fun skills in amateur radio. This intro talk covers everything a beginner needs to know: low cost gear setups, building a simple Yagi antenna, and the techniques used to zero in on a transmitter.

Entry level talk reviewing what foxhunting / radio direction finding is Covering the basic equipment requirements Yagi antenna building Body fading Minimum equipment Tips and tricks

SpeakerBio: Nate Moore

Nate Moore works in cybersecurity, holds an Extra class amateur radio license, and spends his spare time teaching, examining, and pushing signals around the ether.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Ghost Followers: Using AI to Unmask Fake LinkedIn Profiles at Scale

Tags: Packet Hacking Village | Creator Talk/Panel

When: Saturday, Aug 8, 17:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 3 1102 (Creator Stage 6) - [Map](#)

Description:

LinkedIn hosts over 1 billion profiles and a growing number are fake. From AI-generated profile photos to synthetic work histories, adversaries use fake identities for spear-phishing, social engineering, and influence operations. This talk breaks down the anatomy of a fake LinkedIn profile and demonstrates an AI-powered detection framework using behavioral signals, image forensics, and network graph analysis. Attendees will leave with a hands-on methodology and open-source toolset to identify synthetic identities before they become insider threats. Prior knowledge of networking fundamentals is helpful; no machine learning background is required.

SpeakerBio: Aiswarya Venkitesh, Principal Cloud Solution Architect, Microsoft

Aiswarya Venkitesh is a Principal Cloud Solution Architect at Microsoft Canada with 13+ years in Data & AI, specializing in agentic AI architecture, multi-agent orchestration, and enterprise Azure deployments. Ranked #4 globally in IT & Tech by Favikon with 55,000+ LinkedIn followers, she studies identity authenticity and influence operations on professional networks as both a practitioner and creator. She is a confirmed keynote speaker at Futura AI Conference 2026 and author of the forthcoming book The Agentic AI Playbook.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Ghost in the Hiring Machine: How to Spot Fake Personas Before They're on Your Payroll

Tags: Recon Village | Creator Talk/Panel

When: Sunday, Aug 9, 10:00 - 10:45 PDT

Where: LVCCW Level 1 Hall 3 801 (Creator Stage 2) - [Map](#)

Description:

People are getting hired and trusted every day. Some of them do not exist at all, yet they still pass interviews, collect paychecks, and gain access to sensitive systems. Campaigns attributed to the DPRK have shown that this threat is very real. So how do you catch a ghost with a resume? Attendees will learn practical OSINT techniques for spotting fake personas and receive a checklist for thorough background checks. They will see these methods applied through two cases based on a true story, illustrating how these personas succeeded, how one could have been prevented, and where OSINT reaches its limits. These techniques not only help attendees detect fake personas but also provide practical ways to protect their own privacy and control what personal information is visible online.

Speakers: Michael Reimsbach, Rishi "rxerium" C

SpeakerBio: Michael Reimsbach, Product Security Specialist at SAP

Michael is a Product Security Specialist at SAP, working with the SAP Cloud Infrastructure security team. His focus areas include vulnerability management, secrets management, and building secure internal services.

He obtained multiple industry certifications such as OSCP, GCPN, and CISSP.

A healthy dose of paranoia led him to explore OSINT and the surprising power of publicly available information.

Beyond his day-to-day work, Michael is an active member of the cybersecurity community and helps organize BSides Luxembourg.

SpeakerBio: Rishi "rxerium" C, Security Researcher

Rishi is a London-based security researcher with over five years of hands-on experience in IT. He currently specializes in vulnerability research, threat intelligence, and enterprise risk analysis. His current focus lies in identifying and analyzing zero-day vulnerabilities and emerging CVEs, often working to reverse engineer exploit mechanics and build detection logic before public weaponization. Rishi's work spans both offensive and defensive domains—developing threat models based on real-world TTPs, crafting custom detection rules, and automating reconnaissance pipelines to uncover exploitable misconfigurations and exposed assets. He is particularly active in attack surface management (ASM) and OSINT, where he leverages DNS enumeration, passive data correlation, and large-scale infrastructure scanning to surface unknown entry points and map adversary-accessible exposure. Outside of research, Rishi integrates findings into operational tooling and supports data-driven prioritization strategies to bridge technical risk and business impact. His work reflects a deep commitment to adversary-informed defense and proactive discovery across modern hybrid environments.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Ghost in the IDE

Tags: Intro/Beginner | DEF CON Demo Labs | AppSec | Offense/Red Team | DEF CON Demo Labs

When: Friday, Aug 7, 12:00 - 12:45 PDT

Where: LVCCW Level 1 Hall 3 900 (Demo Labs Track 4) - [Map](#)

Description:

Hook: The Blind Spot

Your EDR sees the server compromise. Your SIEM catches the phishing campaign. Your firewall blocks the C2 traffic. But what happens when the attacker doesn't target your infrastructure—they target your developers?

28 million developers worldwide rely on three IDE platforms: JetBrains IntelliJ, Microsoft VS Code, and Eclipse. These aren't just text editors—they're command-and-control platforms disguised as productivity tools. Developers trust them with AWS credentials, database passwords, SSH keys, source code, and network access to production systems. And here's the kicker: IDE plugins run with full user privileges, no sandboxing, no permission dialogs, no questions asked.

We built GHOST IN THE IDE, a production-ready C2 framework that weaponizes IDE plugins across all three major platforms. Not a proof-of-concept. Not a research prototype. A functional red team tool with keystroke logging, clipboard monitoring, file exfiltration, and remote command execution—working silently inside IntelliJ, VS Code, and Eclipse on Windows, macOS, and Linux.

The Attack: Multi-IDE C2 That Actually Works Most IDE plugin research stops at "look, I can pop calc.exe from VS Code." We went further. Way further.

Speakers: Venkata Jayaram Yalla, Pardhiv Reddy

SpeakerBio: Venkata Jayaram Yalla

Yalla, Jayaram is Director – Application Security at S&P Global, leading enterprise-wide initiatives in secure application development, vulnerability management, and security architecture. He has transformed the Application Security function from a primarily tactical penetration-testing team into a strategic security engineering organization, emphasizing automation, governance, and advanced threat modeling.

Jayaram combines deep hands-on experience in offensive security and research (including multiple CVEs) with ownership of large-scale AppSec programs across SAST, SCA, DAST, CI/CD security, and emerging AI security initiatives.

SpeakerBio: Pardhiv Reddy

Pardhiv is a security specialist with vast experience in the field of information security ranging from health care, hospitality, banking and government sectors throughout the world. He also earned many industry standard certifications in the security, some of them are SANS GPEN, OSCP, OSWP, CISSP, Security+, ISO 27001 LA and many others.

Pardhiv's interest areas includes cloud security and IOT security and his research has been presented at EuropeanSec 2016 in Portugal. His expertise helped teams to build secure products and applications by providing security guidelines and best practices.

Pardhiv has performed various IoT security assessments which includes both embedded hardware security, firmware analysis, mobile applications, network security including wireless communications and backend cloud server assessments.

Pardhiv is also an active bug bounty hunter and helped many companies around the world by pointing their security vulnerabilities to make their application and products secure. He spares his free time to build prototypes and security research

by learning new techniques and methodologies.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Ghost in the IDE

Tags: Intro/Beginner | DEF CON Demo Labs | AppSec | Offense/Red Team | DEF CON Demo Labs

When: Saturday, Aug 8, 15:00 - 15:45 PDT

Where: LVCCW Level 1 Hall 3 900 (Demo Labs Track 4) - [Map](#)

Description:

Hook: The Blind Spot

Your EDR sees the server compromise. Your SIEM catches the phishing campaign. Your firewall blocks the C2 traffic. But what happens when the attacker doesn't target your infrastructure—they target your developers?

28 million developers worldwide rely on three IDE platforms: JetBrains IntelliJ, Microsoft VS Code, and Eclipse. These aren't just text editors—they're command-and-control platforms disguised as productivity tools. Developers trust them with AWS credentials, database passwords, SSH keys, source code, and network access to production systems. And here's the kicker: IDE plugins run with full user privileges, no sandboxing, no permission dialogs, no questions asked.

We built GHOST IN THE IDE, a production-ready C2 framework that weaponizes IDE plugins across all three major platforms. Not a proof-of-concept. Not a research prototype. A functional red team tool with keystroke logging, clipboard monitoring, file exfiltration, and remote command execution—working silently inside IntelliJ, VS Code, and Eclipse on Windows, macOS, and Linux.

The Attack: Multi-IDE C2 That Actually Works Most IDE plugin research stops at "look, I can pop calc.exe from VS Code." We went further. Way further.

Speakers: Venkata Jayaram Yalla, Pardhiv Reddy

SpeakerBio: Venkata Jayaram Yalla

Yalla, Jayaram is Director – Application Security at S&P Global, leading enterprise-wide initiatives in secure application development, vulnerability management, and security architecture. He has transformed the Application Security function from a primarily tactical penetration-testing team into a strategic security engineering organization, emphasizing automation, governance, and advanced threat modeling.

Jayaram combines deep hands-on experience in offensive security and research (including multiple CVEs) with ownership of large-scale AppSec programs across SAST, SCA, DAST, CI/CD security, and emerging AI security initiatives.

SpeakerBio: Pardhiv Reddy

Pardhiv is a security specialist with vast experience in the field of information security ranging from health care, hospitality, banking and government sectors throughout the world. He also earned many industry standard certifications in the security, some of them are SANS GPEN, OSCP, OSWP, CISSP, Security+, ISO 27001 LA and many others.

Pardhiv's interest areas include cloud security and IOT security and his research has been presented at EuropeanSec 2016 in Portugal. His expertise helped teams to build secure products and applications by providing security guidelines and best practices.

Pardhiv has performed various IoT security assessments which include both embedded hardware security, firmware analysis, mobile applications, network security including wireless communications and backend cloud server assessments.

Pardhiv is also an active bug bounty hunter and helped many companies around the world by pointing their security vulnerabilities to make their application and products secure. He spares his free time to build prototypes and security research.

by learning new techniques and methodologies.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Ghost in the Water: Simulating a Nation-State PLC Sabotage Campaign

Tags: Red Team Village | Misc

When: Sunday, Aug 9, 14:00 - 14:59 PDT

Where: LVCCW Level 1 Hall 1 309 (Red Team Village) Tactic Table 4 - [Map](#)

Description:

Critical infrastructure protocols designed in the late 70s were never built to handle a modern adversary. In this hands-on Tactic, we move beyond theoretical slides to execute a high-fidelity, nation-state-style operation against a municipal water treatment facility. Using a portable Software-in-the-Loop (SiL) environment, participants will experience the raw tradecraft of industrial sabotage without the need for a six-figure hardware rack.

This session focuses on "Living-off-the-Ladder" (LotL)—the art of using legitimate industrial function codes to perform unauthorized actions. You will not be dropping malware; you will be programmatically manipulating the physics of the plant using the same TTPs seen in recent geopolitical conflicts.

The Mission (30–60 Minute Sprint):

Industrial Interrogation: Use unauthenticated DNP3 and S7comm discovery to fingerprint PLCs and map the process logic—capturing vendor data and firmware versions silently.

The Memory Heist: Execute a "Credential Harvest" (T0861) by programmatically reading PLC holding registers to recover plaintext maintenance keys.

Coordinated Sabotage: Trigger a "Slow-and-Low" chemical setpoint override (Modbus FC16) across multiple facilities simultaneously, observing real-time physical feedback from the simulated plant sensors. • Phase 1: Automated multi-protocol fingerprinting and asset discovery. • Phase 2: Executing a "Memory Heist" to extract plaintext maintenance credentials directly from PLC registers. • Phase 3: A coordinated "Slow-and-Low" chemical setpoint override, providing real-time visual feedback of the physical process failure.

Attendee Takeaway: Participants will build the muscle memory required to navigate OT environments and will leave with a deployable, containerized SiL framework to continue their own ICS research and detection validation at home. Attendees will leave with a deployable SiL framework and the "Living-off-the-Ladder" playbook to continue their own ICS research without the need for expensive hardware.

Speakers: Blessen Thomas, Javier Hernández, Wojciech Poparda

SpeakerBio: Blessen Thomas

Blessen Thomas is an Independent Security Researcher. He has more than 13+ years of experience in Red Teaming, Appsec (Web, Thick, API & Mobile Apps), Smart Watch Wearable Application Penetration Testing, Mobile Penetration Test (iOS, Android, Windows platform), IoT, OT, mainframes, SAP, SWIFT, RPA, Cloud, ATM, KIOSK, Vulnerability Assessment and Network Penetration Test, Physical Covert Entry, Wireless assessments, Telecom (2G, 3G, USSD) etc. for several enterprise companies and financial institutions all across the globe. He is a B.Tech in Information Technology from Anna University and holds industry certifications such as SANS GPEN, CRTO, OPST, CREST CRT(PEN), CREST CPSA, OSCP, CRTP, OSWP, C)PTE, CEH, CHFI. He has been listed and acknowledged in various "HALL OF FAMES" for various companies such as Oracle, Sony, Kayako, Appcclerator, Hotgloo, Meldium, Splunk and many more for responsible disclosure. He has been a bug bounty hunter and contributor for the OWASP Mobile Testing Guide Project (MSTG), Tamer OS, Seclists, OWASP top 10 API, OSSTMM, Awesome Mainframe Hacking, RvR, WAVSEP Benchmark sectool projects. His research training/talks has been accepted into various security conferences like Hack in the Box-Dubai, Haktivity -Hungary, CanSecWest -Canada, OWASP Appsec EU- London -UK, OWASP Appsec Europe-Italy, RootCon-Philippines, OWASP

PH,OWASP New Zealand Day, Infosec SouthWest,Austin,Texas, FSec-Croatia, Hackbeach, Hackfest, Shakacon,ITWeb-South Africa, Jordan Cyber Security Summit, HITCON-Taiwan, OWASP AppSec-Bucharest, OWASP Appsec Africa-Morocco,CircleCityCon,OWASP Botswana,CactusCon,Bsides-London,Prishtina,Aarhus,Vilnius,Elbsides,Kristiansand,Athens and many more. He has been invited as Speaker for Radio Talk Shows for All India Radio. He spends his leisure time playing drumkit and percussion.

SpeakerBio: Javier Hernández

Javier is a Red Team Operator and Malware Developer specializing in offensive engineering, adversary emulation, and custom tooling development. Holding certifications such as OSEP and CRT0, he has delivered high impact security engagements across both consulting environments and in house security teams. His work focuses on crafting stealthy implants, evasion techniques, and automation driven offensive capabilities. Passionate about applied research, he explores the intersection of malware development and AI augmented offensive security to help organizations strengthen their resilience against modern threats

SpeakerBio: Wojciech Poparda

Wojciech Poparda is a cybersecurity consultant. He helps organizations proactively defend their digital infrastructure by thinking like an adversary. Leveraging a deep foundation in Offensive Security, he specializes in designing resilient Security Architectures that bridge the gap between complex attack vectors and enterprise defense, with a sharp focus on Cloud Security and Identity & Access Management (IAM).

His approach is backed by rigorous technical validation, holding industry-leading certifications including OSCP, CRTE, CRTP, CRT0, CPTS, CWES, AWS Certified Solutions Architect - Associate and AWS Certified Security - Specialty. He is also an Associate of ISC2, having successfully passed the CISSP exam.

Beyond the terminal, he channels the discipline, focus, and resilience required for cybersecurity into his life as a triathlete. As an IRONMAN European and World Championships finisher, he brings the same endurance and dedication to solving complex security challenges as he does to the race course.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Ghost Records: Automating Dangling DNS & Subdomain Takeover Detection at Enterprise Scale

Tags: Cloud Village | Creator Talk/Panel

When: Saturday, Aug 8, 10:40 - 11:20 PDT

Where: LVCCW Level 3 W313 (Cloud Village Talks) - [Map](#)

Description:

This is not another subdomain takeover 101 talk. It's about what dangling DNS actually looks like at enterprise scale - in large, multi-account AWS environments with sprawling DNS footprints - and the automation and hard-won triage lessons the problem demands.

Let's be honest: ~95% of subdomain takeover findings are noise - 3rd- and 4th-level subdomains on dead non-prod environments no customer ever visits. They generate alert fatigue and little else. The other 5% - cookie theft via a *.domain.com scope, OAuth token hijack, phishing from a legitimate domain carrying a valid TLS cert - are catastrophic. Telling the 5% from the 95% is the entire game.

Then there's the bug bounty dynamic. Researchers find these in bulk and report them in bulk. They're frustrated that fixes take weeks; program owners are frustrated that most reports are low-impact but can't simply be closed. The relationship erodes on both sides - a cost nobody puts on a dashboard.

From what We've seen, the time sinks are predictable: manually triaging hundreds of researcher reports, chasing low-impact findings, writing one-off fix scripts instead of systemic solutions, and reconstructing record ownership after the fact. The structural causes are just as consistent: multi-account sprawl with no central DNS ownership, rapid dev cycles where IaC teardowns never touch Route53, and researchers reporting faster than teams can remediate.

The core of the talk is architecture: automatically cross-referencing every Route53 A record and CNAME against Elastic IPs allocated across all AWS regions, wired into ownership routing and shift-left pipeline hooks. Done right, this shifts detection from reactive to proactive, can take MTTR from weeks to hours, and eliminates entire classes of records at the source.

We'll release Ghost Records, an open-source tool aimed at the one of the highest impact vector: dangling A records and CNAMEs pointing to released or unallocated AWS Elastic IPs. It inventories every EIP across all enabled regions, cross-references them against Route53, and flags any DNS record pointing to an IP the account doesn't own. Read-only, multi-account, parallel scanning, risk-scored output. Live demo included.

Speakers: Jai Kumar Sharma, Tom McCarthy

SpeakerBio: Jai Kumar Sharma, Principal Offensive Security Engineer at GoDaddy

Jai Sharma is a Principal Offensive Security Engineer at GoDaddy, where he leads cloud penetration testing, red team operations, AI red teaming, and security research across one of the world's largest domain registrars and hosting platforms. A self-taught offensive security researcher from New Delhi, India, he built his career with a hacker's mindset, breaking code logic, chasing vulnerabilities, and proving real-world business impact from technical exploits. He also leads TTP research, drives threat emulation efforts, and works closely with blue teams to sharpen detection through an adversary-focused lens.

At GoDaddy, Jai tests the same infrastructure and enterprise environments that millions of customers rely on. His work spans cloud and on-premises penetration testing, IAM privilege escalation research, and building automated offensive tooling that helps turn point-in-time assessments into continuous detection. Before GoDaddy, Jai held offensive security roles at Housing.com, FIS, and EY, giving him firsthand experience with how security weaknesses and misconfigurations surface across different industries, architectures, and maturity levels.

Jai volunteers with the DEF CON community as CTF Ops for the Cloud Village and on-site Coordinator for the Bug Bounty Village.

SpeakerBio: Tom McCarthy

Tom McCarthy is the Director of Offensive Security and Business Information Security Officer at GoDaddy, where he oversees penetration testing, red team operations, and security strategy across multiple lines of business. With over 15 years in offensive security — spanning consulting, penetration testing, research, and training — Tom has built multiple penetration testing teams from the ground up and led or managed hundreds of penetration tests and red team engagements throughout his career. Tom is a returning DEF CON speaker, having previously presented research, tooling, and training at both DEF CON and DerbyCon. He has contributed to open-source offensive security projects including smbexec and Metasploit, and served as a trainer in hacking and incident response for local, federal, and military organizations across multiple countries.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: GhostCatcher (endpoint detection agent)

Tags: DEF CON Demo Labs | Intermediate | Defense/Blue Team | Purple Team | DEF CON Demo Labs

When: Saturday, Aug 8, 11:00 - 11:45 PDT

Where: LVCCW Level 1 Hall 3 1001 (Demo Labs Track 1) - [Map](#)

Description:

GhostCatcher is an open-source Linux endpoint detection agent written in Go. It runs as a single binary or a systemd service and looks for host-visible adversary tradecraft on Linux: web shells, LD_PRELOAD abuse, SSH, cron, and systemd persistence, PAM/sudoers tampering, SUID and capability drift, reverse shells and unexpected network behavior, reflective / memory-map signals, and related patterns aligned with MITRE ATT&CK-style coverage. Detections are driven by a versioned, optionally signed rule pack, baselines and learning mode, multi-signal scoring, time-windowed correlation, CEL-style boolean expressions, optional Sigma-lite rules, optional YARA (disk and memory) and eBPF (with auditd/proc fallbacks), and JSONL output to stdout plus optional syslog, Splunk HEC, Elasticsearch _bulk, or Grafana Loki. The goal is to give blue teams a transparent, self-hosted way to turn Linux host telemetry into actionable events in the SIEM—without a vendor cloud control plane.

SpeakerBio: Sercan Okur

Sercan Okur is the Founder and CEO of NextRay AI Detection & Response, Inc., a San Jose-based cybersecurity company building AI-driven Network Detection and Response technology. A cybersecurity practitioner with more than fifteen years of experience across critical-infrastructure, defense, and enterprise environments,

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: GhostCatcher (endpoint detection agent)

Tags: DEF CON Demo Labs | Intermediate | Defense/Blue Team | Purple Team | DEF CON Demo Labs

When: Friday, Aug 7, 15:00 - 15:45 PDT

Where: LVCCW Level 1 Hall 3 1001 (Demo Labs Track 1) - [Map](#)

Description:

GhostCatcher is an open-source Linux endpoint detection agent written in Go. It runs as a single binary or a systemd service and looks for host-visible adversary tradecraft on Linux: web shells, LD_PRELOAD abuse, SSH, cron, and systemd persistence, PAM/sudoers tampering, SUID and capability drift, reverse shells and unexpected network behavior, reflective / memory-map signals, and related patterns aligned with MITRE ATT&CK-style coverage. Detections are driven by a versioned, optionally signed rule pack, baselines and learning mode, multi-signal scoring, time-windowed correlation, CEL-style boolean expressions, optional Sigma-lite rules, optional YARA (disk and memory) and eBPF (with auditd/proc fallbacks), and JSONL output to stdout plus optional syslog, Splunk HEC, Elasticsearch _bulk, or Grafana Loki. The goal is to give blue teams a transparent, self-hosted way to turn Linux host telemetry into actionable events in the SIEM—without a vendor cloud control plane.

SpeakerBio: Sercan Okur

Sercan Okur is the Founder and CEO of NextRay AI Detection & Response, Inc., a San Jose-based cybersecurity company building AI-driven Network Detection and Response technology. A cybersecurity practitioner with more than fifteen years of experience across critical-infrastructure, defense, and enterprise environments,

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Github Rate Limits Got You Down? FOD's Failing to Build? Let's Talk About Caching

Tags: Nix Vegas Community | Creator Talk/Panel

When: Friday, Aug 7, 16:45 - 16:59 PDT

Where: LVCCW Level 1 Hall 4 1310 (Nix Vegas Community) - [Map](#)

Description:

Have you ever experienced being rate limited by GitHub? Has GitHub downtime prevented you from building software that you rely on? Are you worried about supply chain attacks? At Exa, we developed a secure, hostable, tarball cache that insulates us from GitHub outages, decreases our build times, protects us from force-pushes upstream, and increases download speeds.

SpeakerBio: Ethan Carter Edwards

Ethan is a FLOSS advocate, longtime Nix user and contributor, and engineer. He's an active member of the Nixpkgs CUDA, Darwin, and NGI teams and is involved in various other efforts throughout the Nix ecosystem.

He currently works on building the infrastructure for the future of websearch at Exa.ai and studies Computer Science at Harvard University.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Give an AI Industrial Protocol Tools and Watch What It Destroys

Tags: ICS Village | Creator Talk/Panel

When: Saturday, Aug 8, 14:45 - 15:30 PDT

Where: LVCCW Level 1 Hall 3 801 (Creator Stage 1) - [Map](#)

Description:

Every major ICS attack of the last decade succeeded not because of software vulnerabilities, but because industrial protocols were built to trust any packet on the wire. The village has read the incident reports. What it doesn't have is a way to replay them against its own infrastructure to learn what its detections actually catch and what they miss.

We present mrhOTshOT, an open-source framework that emulates history's most destructive ICS attacks across the complete kill chain, reconstructed from publicly available incident analyses. Not just the OT payload the full chain: Windows initial access with real CVEs, lateral movement to engineering workstations, protocol-native process manipulation, and persistent physical impact. Every emulation generates wire traffic consistent with publicly documented behavior on the correct industrial protocol for that attack family.

The framework spans a wide range of industrial protocols across ten distributed PLCs, each simulating the real-world process that protocol actually controls: a heating district controller for Modbus, a safety instrumented system for TriStation, a centrifuge cascade for S7comm. Nothing runs on a generic simulated tank with ten protocols bolted on.

We also introduce the Agentic Attack Emulation Framework: every protocol action is exposed as a callable tool, orchestrated by an LLM agent that reads live process state and composes attack sequences on the fly. No hardcoded playbook, you decide. This is what AI-assisted ICS attack composition looks like, and defenders need to understand it before they meet it in the wild.

The talk closes with a live demo: three centrifuges destroyed in real time while the operator HMI, deceived by an S7 rootkit, shows normal operation throughout, until it doesn't.

Speakers: Malav Vyas, Asher Davila

SpeakerBio: Malav Vyas, Palo Alto Networks

OT and IoT security researcher. I spend my time hunting vulnerabilities, crafting exploits, and pushing the boundaries of ecosystem security. When I'm not breaking things, I'm helping run the show with the Null, BSides, and OWASP communities. Catch me at the villages.

SpeakerBio: Asher Davila, Vulnerability Researcher at Palo Alto Networks

Passionate about binary analysis, binary exploitation, reverse engineering, hardware hacking, retro computing, and music.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Contests - Saturday - 12:00-15:59 PDT

Title: Global OSINT Search Party CTF – DEF CON 34 Edition

Tags: OSINT For Good Community | Contest

When: Saturday, Aug 8, 12:00 - 15:59 PDT

Where: LVCCW Level 1 Hall 4 1307 (OSINT4Good Community) - [Map](#)

Description:

The Trace Labs Global OSINT Search Party CTF is a non-theoretical CTF where teams of up to 4 people use their OSINT skills to look for actual missing people. For DEF CON 34, we will be working directly with Las Vegas Metro PD to source local missing person cases they have requested the public's assistance with. This is a hybrid event, open to participants of all skill levels, from anywhere in the world. Prizes will be awarded for 1st, 2nd, and 3rd places, as well as for Most Valuable OSINT. Participants at DEF CON can pickup their free event ticket by stopping by the OSINT4Good Community anytime prior to the event start. Global participants can get a ticket by going to <https://www.tracelabs.org/tickets>. Bring a laptop and some snacks and get ready to use OSINT4Good!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: GnawLab: Open-Source AWS Attack Scenarios Based on Real-World Breaches

Tags: Intro/Beginner | AI | DEF CON Demo Labs | Cloud | Offense/Red Team | DEF CON Demo Labs

When: Saturday, Aug 8, 16:00 - 16:45 PDT

Where: LVCCW Level 1 Hall 3 1002 (Demo Labs Track 2) - [Map](#)

Description:

GnawLab is a community-driven, open-source offensive cloud security training platform that recreates real-world AWS attack chains. Each scenario is modeled after documented breaches—Capital One's SSRF-to-IMDS pivot, Uber's leaked credential exploitation, SolarWinds-style CI/CD pipeline hijacking—deployed via Terraform in your own AWS account. Attendees will see live demonstrations of multi-hop attack chains: from SSRF and command injection entry points, through IMDS credential theft and Secrets Manager extraction, to full CI/CD pipeline compromise with Blue/Green deployment backdoors. GnawLab bridges the gap between theoretical cloud security knowledge and hands-on exploitation skills.

Speakers:ialleejy,Kyul,HyunJun "Beaver King" Kwon

SpeakerBio: ialleejy

I am ialleejy, a Security Researcher at ENKI focusing on web security and cloud security. I have created WEB challenges for CODEGATE and HACKTHEON SEJONG CTF, and I am interested in designing CTF challenges that connect real-world service architectures with practical vulnerability research.

Recently, I have been exploring Offensive Cloud Security, especially how traditional web vulnerabilities can lead to privilege escalation, credential exposure, and abuse of trust relationships in cloud environments. I am currently diving deeper into AWS Bedrock AI Agents, RAG-based knowledge poisoning, OIDC authentication flows, and IAM trust policies.

Through this talk, I aim to show how a small vulnerability on the web can evolve into a broader cloud security issue, crossing trust boundaries between applications, identities, and cloud services.

SpeakerBio: Kyul

I am a college student relentlessly exploring cloud vulnerabilities. I possess an exceptionally high threshold for hunting, gathering, and deeply analyzing whatever piques my interest.

My mindset is clear: effective defense demands an attacker's lens. Only by understanding actual infiltration paths and how they trigger critical risks can defenders accurately prioritize assets and build robust controls.

Driven by this, I've operated at the intersection of Red and Blue. In incident response projects, I analyzed real-world TTPs to build attack scenarios while collaborating to engineer detection rules and automated responses. I've also researched and presented how AWS misconfigurations can be weaponized to cause cascading breaches.

Currently, alongside the BeaverDam community, I am developing GnawLab for the DEF CON Demo Lab. GnawLab is an open-source, community-driven cloud security training platform. It provides high-fidelity sandbox environments reflecting real-world flaws, enabling players to execute realistic scenarios and vividly master cloud exploitation and analysis.

At DEFCON, my goal isn't just to show what I've built. I want to share this sandbox, break it alongside you, and absorb the brilliant, diverse approaches of world-class hackers. I am here to hack, learn, and grow together.

SpeakerBio: HyunJun "Beaver King" Kwon

HyunJun Kwon is an Application and Cloud Security Engineer with 12 years of offensive security experience. Currently at Rapport Labs in Korea, he previously led vulnerability assessments, DevSecOps, and cloud security initiatives at Woowa Brothers, the company behind Baemin, South Korea's largest food delivery platform.

He serves as an AWS Community Builder for security and leads the Beaver Dam Community, an offensive cloud security research group. He also contributes to AWS Bedrock Agent Samples and mentors junior security professionals through programs like Baby Beavers, K-Shield Junior, and Whitehat School.

His cloud security research focuses on scaling security in dynamic environments. He built automated CCE assessment systems using AWS VPC Endpoints and Systems Manager. Recently he explored AI and security intersections, building LangChain and LangGraph agents for infrastructure assessment automation and MCP security checkers to detect supply chain risks.

He won the 2021 HDCON Grand Prize for cloud security architecture and authored two books on web hacking. He spoke at .HACK 2025 on Offensive Cloud Security and at .HACK 2026 on whether CloudTrail and GuardDuty are really enough.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: GnawLab: Open-Source AWS Attack Scenarios Based on Real-World Breaches

Tags: Intro/Beginner | AI | DEF CON Demo Labs | Cloud | Offense/Red Team | DEF CON Demo Labs

When: Friday, Aug 7, 12:00 - 12:45 PDT

Where: LVCCW Level 1 Hall 3 1002 (Demo Labs Track 2) - [Map](#)

Description:

GnawLab is a community-driven, open-source offensive cloud security training platform that recreates real-world AWS attack chains. Each scenario is modeled after documented breaches—Capital One's SSRF-to-IMDS pivot, Uber's leaked credential exploitation, SolarWinds-style CI/CD pipeline hijacking—deployed via Terraform in your own AWS account. Attendees will see live demonstrations of multi-hop attack chains: from SSRF and command injection entry points, through IMDS credential theft and Secrets Manager extraction, to full CI/CD pipeline compromise with Blue/Green deployment backdoors. GnawLab bridges the gap between theoretical cloud security knowledge and hands-on exploitation skills.

Speakers:ialleejy,Kyul,HyunJun "Beaver King" Kwon

SpeakerBio: ialleejy

I am ialleejy, a Security Researcher at ENKI focusing on web security and cloud security. I have created WEB challenges for CODEGATE and HACKTHEON SEJONG CTF, and I am interested in designing CTF challenges that connect real-world service architectures with practical vulnerability research.

Recently, I have been exploring Offensive Cloud Security, especially how traditional web vulnerabilities can lead to privilege escalation, credential exposure, and abuse of trust relationships in cloud environments. I am currently diving deeper into AWS Bedrock AI Agents, RAG-based knowledge poisoning, OIDC authentication flows, and IAM trust policies.

Through this talk, I aim to show how a small vulnerability on the web can evolve into a broader cloud security issue, crossing trust boundaries between applications, identities, and cloud services.

SpeakerBio: Kyul

I am a college student relentlessly exploring cloud vulnerabilities. I possess an exceptionally high threshold for hunting, gathering, and deeply analyzing whatever piques my interest.

My mindset is clear: effective defense demands an attacker's lens. Only by understanding actual infiltration paths and how they trigger critical risks can defenders accurately prioritize assets and build robust controls.

Driven by this, I've operated at the intersection of Red and Blue. In incident response projects, I analyzed real-world TTPs to build attack scenarios while collaborating to engineer detection rules and automated responses. I've also researched and presented how AWS misconfigurations can be weaponized to cause cascading breaches.

Currently, alongside the BeaverDam community, I am developing GnawLab for the DEF CON Demo Lab. GnawLab is an open-source, community-driven cloud security training platform. It provides high-fidelity sandbox environments reflecting real-world flaws, enabling players to execute realistic scenarios and vividly master cloud exploitation and analysis.

At DEFCON, my goal isn't just to show what I've built. I want to share this sandbox, break it alongside you, and absorb the brilliant, diverse approaches of world-class hackers. I am here to hack, learn, and grow together.

SpeakerBio: HyunJun "Beaver King" Kwon

HyunJun Kwon is an Application and Cloud Security Engineer with 12 years of offensive security experience. Currently at Rapport Labs in Korea, he previously led vulnerability assessments, DevSecOps, and cloud security initiatives at Woowa Brothers, the company behind Baemin, South Korea's largest food delivery platform.

He serves as an AWS Community Builder for security and leads the Beaver Dam Community, an offensive cloud security research group. He also contributes to AWS Bedrock Agent Samples and mentors junior security professionals through programs like Baby Beavers, K-Shield Junior, and Whitehat School.

His cloud security research focuses on scaling security in dynamic environments. He built automated CCE assessment systems using AWS VPC Endpoints and Systems Manager. Recently he explored AI and security intersections, building LangChain and LangGraph agents for infrastructure assessment automation and MCP security checkers to detect supply chain risks.

He won the 2021 HDCON Grand Prize for cloud security architecture and authored two books on web hacking. He spoke at .HACK 2025 on Offensive Cloud Security and at .HACK 2026 on whether CloudTrail and GuardDuty are really enough.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Go with the Flow: Riding GCP Dataflow Shadow Dependency to Cross-Tenant Compromise

Tags: Cloud Village | Creator Talk/Panel

When: Friday, Aug 7, 15:10 - 15:30 PDT

Where: LVCCW Level 3 W313 (Cloud Village Talks) - [Map](#)

Description:

Cloud resources rely on a web of trust that most security teams ignore. Even if you secure access to a resource, you might miss its "shadow dependencies" - the external, system-generated resources required for it to function.

GCP Dataflow is just the latest in a long trail of vulnerable services suffering from this architectural blind spot. What we found is a fundamental flaw in how Dataflow blindly trusts dependencies located far outside its IAM control and security boundaries.

In this talk, we'll present two novel attack techniques that weaponize unvalidated config files to hijack trusted data pipelines. We'll also demonstrate a critical cross-tenant vulnerability that extends this issue by enabling manipulation of Dataflow orchestration across tenant boundaries. The issue remains under responsible disclosure and is expected to be fixed before the presentation.

Background: GCP Dataflow and Managed Infrastructure

Organizations running large-scale enterprise data workloads increasingly rely on managed data-processing services, especially GCP Dataflow. Built on Apache Beam, Dataflow executes unified data pipelines while removing much of the operational burden of provisioning cluster frameworks, tuning virtual machines, and scaling infrastructure in response to demand. Teams define the pipeline, and Dataflow provisions and scales the underlying compute resources automatically.

During this orchestration, however, Dataflow pipelines often depend on objects stored in standard cloud storage buckets to control execution, such as code, templates, and environment configuration.

Pipelines routinely ingest and execute files from cloud buckets, including JavaScript or Python User Defined Functions (UDFs) for runtime transformation, structured YAML job templates that define pipeline parameters, and other environment configuration files.

Because these files and their supporting temporary assets are often managed through automated developer pipelines, they can become "shadows": overlooked in routine asset inventories and security posture reviews, yet still critical to the execution of highly trusted cloud workflows.

Key Takeaways

Dismantling the shadow resources blind spot: Understand how automated cloud orchestration creates short-lived access windows that can evade scheduled security scans and routine asset inventories.

Auditing the infrastructure-as-config attack surface: Learn to treat external execution blueprints as active attack surfaces rather than passive configuration files.

Applying defensive best practices: Take away architectural recommendations for designing pipelines that are more resilient to these attack paths.

Session Details

Total duration: 20 minutes

5 minutes: Background on shadow resources and Dataflow mechanics.

10 minutes: Walkthrough of the attack paths and the cross-tenant vulnerability.

5 minutes: Research methodology, defensive takeaways, and detection strategies.

Speakers: Gil Weizman, Tamir Yehuda

SpeakerBio: Gil Weizman

Gil Weizman is an experienced security researcher with over ten years of expertise across on prem, cloud, web, and SaaS security. Gil focuses on threat detection, product security research, vulnerability research and identifying gaps in security visibility across modern environments. Gil specializes in translating real world attacker behavior into improved detection and mitigation strategies.

SpeakerBio: Tamir Yehuda

Tamir Yehuda is a Senior Security Researcher and cloud security team lead at Varonis. He is a full-stack hacker with experience in malware analysis, Windows & AD domains, SaaS applications, and cloud infrastructure. Tamir specialize in IaaS & PaaS research focusing mainly on Azure, GCP, AWS, Salesforce, and ServiceNow. He brings over eight years of experience in various types of security research and red teaming.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Going the Distance: Long-Range Keystroke Injection via Meshtastic

Tags: DEF CON Official Talk | Demo | Tool

When: Sunday, Aug 9, 10:00 - 10:30 PDT

Where: LVCCW Level 1 Hall 3 904 (Main Track 4) - [Map](#)

Description:

What if your keystroke injection implant could be triggered from kilometers away, through walls, without WiFi, cellular, or line-of-sight? What if the entire Meshtastic network relayed your commands for you? M.I.A. (Mesh Injection Apparatus) is a new open-source offensive tool that combines USB HID injection with LoRa mesh networking. Plant a device during brief physical access, then trigger payloads remotely- across a building, a campus, or a city, using Meshtastic's encrypted mesh protocol. No internet required. No WiFi range limitations. Just long-range, low-power radio that blends into the growing ecosystem of LoRa devices. This talk covers the complete build: understanding USB HID at the protocol level, reverse-engineering Meshtastic's packet structure and AES-CTR encryption, implementing a DuckyScript parser from scratch in C++, and designing custom PCB hardware. I'll demonstrate remote-triggered injection over the mesh network, discuss operational considerations for red teams, and release all firmware, schematics, and tooling as open source. MIA represents a new class of implant, one that stays connected when traditional C2 channels fail.

<https://www.blackhillsinfosec.com/introducing-lora-long-range-wireless-technology-part-1/>

(I would like to cite Venky Raju's talk, but I could not find it online. I will try to reach out to him.)

SpeakerBio: Benito "paperclipsvinny" Saucedo

Benito Saucedo is a 19-year-old university student who saw a talk at a small regional conference, got inspired, and spent the next few months procrastinating homework to build his own version from scratch. It escalated quickly.

His proudest accomplishments stem mostly from growing cybersecurity communities, a curious side effect of talking about hacking with everyone around him. He founded cybersecurity clubs at both his high school and local community college, taught cybersecurity to 8–12th grade students through the Bay Area Cyber League, and helped develop regional cybersecurity competitions for 16 Bay Area community colleges.

This is his first DEF CON talk.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Crypto & Privacy Village - Saturday - 11:00-11:59 PDT

Title: Gold Bug: Puzzle Panel with Friends

Tags: Crypto & Privacy Village | Creator Talk/Panel

When: Saturday, Aug 8, 11:00 - 11:59 PDT

Where: LVCCW Level 1 Hall 3 1102 (Creator Stage 6) - [Map](#)

Description:

Speakers:CPV Gold Bug Team 2026,TBD

SpeakerBio: CPV Gold Bug Team 2026

No BIO available

SpeakerBio: TBD

No BIO available

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Gone in 60 Frames – USB Video Exploitation

Tags: DEF CON Official Talk | Demo | Exploit

When: Sunday, Aug 9, 11:00 - 11:59 PDT

Where: LVCCW Level 1 Hall 3 903 (Main Track 5) - [Map](#)

Description:

In 2025, Amnesty International, in collaboration with Google TAG, released a write-up of an in-the-wild chain of USB Linux kernel vulnerabilities which was used to compromise mobile devices.

Whilst the vulnerabilities themselves were disclosed, no details on how these vulnerabilities could be exploited were provided. This led us to deep dive into these issues to determine how they could be leveraged for arbitrary code execution.

This is the story of exploiting one of these vulnerabilities (CVE-2024-53104), an out of bounds write in USB Video which offered a brilliant exploit primitive leading to highly reliable code execution when chained together with an information leakage vulnerability.

In this talk we will first discuss the in-the-wild vulnerabilities, moving on to providing background of USB specifics for several device classes and coverage guided fuzzing for finding new issues.

We will then move onto a more recent information disclosure vulnerability CVE-2025-38494 which could be leveraged to bypass KASLR.

An extensive deep dive into CVE-2024-53104 vulnerability will be performed (the OOB write) and we will discuss our novel technique used for exploitation of this issue and expose the power of the UVC_QUIRK_RESTRICT_FRAME_RATE quirk!

Finally, we will wrap up our talk with several demonstrations.

Speakers: Alex Plaskett, Robert Herrera

SpeakerBio: Alex Plaskett, NCC Group

Alex Plaskett (@alexjplaskett) is an Associate Director within the Exploit Development Group (EDG) at NCC Group. Alex is a five-time Pwn2Own winner (desktop, mobile, embedded, and automotive) and has over 16+ years of experience in vulnerability research and exploitation. Alex has exploited vulnerabilities in a large range of high-profile products across many different areas of security. Alex is a frequent speaker at security conferences (e.g. BlackHat, OffensiveCon, Hexacon, HITB, BlueHat, POC, Troopers etc). Alex was previously leading security teams in Fintech, Mobile Security and Security Research) and just generally causing vendors to patch things on a regular basis!

SpeakerBio: Robert Herrera, NCC Group

Robert Herrera (@robert.herrera_) is a Lead Security Researcher within the Exploit Development Group (EDG) at NCC Group. Robert has extensive experience performing high-impact security audits and reverse-engineering for a diverse set of technologies ranging from automotive, modems, secure boot platforms, and wireless technologies. Robert has 9+ years of experience and has worn many hats over the years ranging from iOS Developer, Software Engineer, to Reverse Engineer.

Title: Goose Processing Unit (GPU): VRAM as an Unmonitored Attack Surface

Tags: DEF CON Demo Labs | Intermediate | Defense/Blue Team | Hardware/IoT | Malware | Offense/Red Team | DEF CON Demo Labs

When: Saturday, Aug 8, 10:00 - 10:45 PDT

Where: LVCCW Level 1 Hall 3 1003 (Demo Labs Track 3) - [Map](#)

Description:

Modern GPUs have become foundational to computing infrastructure for gaming, machine learning, and AI workloads at scale, yet GPU memory remains a largely unmonitored attack surface. No mainstream antivirus or endpoint-detection solution currently inspects it, creating a significant blind spot that sophisticated adversaries can exploit. This Demo Lab presents a novel technique that uses NVIDIA RTX 5090 CUDA APIs to stage payload data, such as DLLs, directly in GPU memory, entirely outside the visibility of host-based security tools, including Windows Defender. A benign executable, with no malicious code of its own, uses CUDA's native memory transfer capabilities to move binary payload data onto the GPU immediately upon execution. No CUDA Toolkit installation is required on the target host. When triggered, the same executable retrieves the payload from GPU memory, manually maps it into process space, and executes it. A working proof of concept has been validated as an Empire C2 module, confirming practical operational viability. The technique is particularly impactful for high-uptime environments such as AI inference servers, rendering farms, and enterprise GPU clusters, where small executables interacting with the GPU blend naturally into background workloads.

Speakers: Gannon "Dorf" Gebauer, Anthony "Coin" Rose, Hana Christensen

SpeakerBio: Gannon "Dorf" Gebauer

Gannon "Dorf" Gebauer is a second lieutenant in the United States Air Force pursuing a master's in computer science at the Air Force Institute of Technology. He earned a Bachelor of Science in Computer Science from Arizona State University. His expertise spans red team operations, reverse engineering, and offensive tool development, and his current research focuses on novel persistence techniques that abuse GPU memory as an unmonitored attack surface.

SpeakerBio: Anthony "Coin" Rose

Dr. Anthony "Coin" Rose is an officer in the United States Air Force, an Assistant Professor, and the Director of the Center for Cyberspace Research at the Air Force Institute of Technology. He holds a doctorate in Electrical Engineering and has expertise in machine learning, with a focus on its application to cybersecurity and malware detection. He is also the founder of SIMAPTIC and the Director of Security Research at BC Security, where he specializes in adversary tactics and emulation planning, Red and Blue Team operations, and embedded systems security. Dr. Rose is credited with 16 CVEs and has presented at numerous security conferences, including Black Hat, DEF CON, HackSpaceCon, HackMiami, and RSA Conference.

SpeakerBio: Hana Christensen

Hana Christensen is a second lieutenant and developmental engineer (electrical) in the United States Air Force. She is currently pursuing a master's in electrical engineering, with a focus on signal processing and machine learning. Her research investigates security vulnerabilities in AI hardware, examining whether side-channel analysis can be used to extract information about machine learning algorithms. She holds a B.S. in Electrical and Computer Engineering from the United States Air Force Academy (class of 2025).



Title: Goose Processing Unit (GPU): VRAM as an Unmonitored Attack Surface

Tags: DEF CON Demo Labs | Intermediate | Defense/Blue Team | Hardware/IoT | Malware | Offense/Red Team | DEF CON Demo Labs

When: Friday, Aug 7, 13:00 - 13:45 PDT

Where: LVCCW Level 1 Hall 3 1003 (Demo Labs Track 3) - [Map](#)

Description:

Modern GPUs have become foundational to computing infrastructure for gaming, machine learning, and AI workloads at scale, yet GPU memory remains a largely unmonitored attack surface. No mainstream antivirus or endpoint-detection solution currently inspects it, creating a significant blind spot that sophisticated adversaries can exploit. This Demo Lab presents a novel technique that uses NVIDIA RTX 5090 CUDA APIs to stage payload data, such as DLLs, directly in GPU memory, entirely outside the visibility of host-based security tools, including Windows Defender. A benign executable, with no malicious code of its own, uses CUDA's native memory transfer capabilities to move binary payload data onto the GPU immediately upon execution. No CUDA Toolkit installation is required on the target host. When triggered, the same executable retrieves the payload from GPU memory, manually maps it into process space, and executes it. A working proof of concept has been validated as an Empire C2 module, confirming practical operational viability. The technique is particularly impactful for high-uptime environments such as AI inference servers, rendering farms, and enterprise GPU clusters, where small executables interacting with the GPU blend naturally into background workloads.

Speakers: Gannon "Dorf" Gebauer, Anthony "Coin" Rose, Hana Christensen

SpeakerBio: Gannon "Dorf" Gebauer

Gannon "Dorf" Gebauer is a second lieutenant in the United States Air Force pursuing a master's in computer science at the Air Force Institute of Technology. He earned a Bachelor of Science in Computer Science from Arizona State University. His expertise spans red team operations, reverse engineering, and offensive tool development, and his current research focuses on novel persistence techniques that abuse GPU memory as an unmonitored attack surface.

SpeakerBio: Anthony "Coin" Rose

Dr. Anthony "Coin" Rose is an officer in the United States Air Force, an Assistant Professor, and the Director of the Center for Cyberspace Research at the Air Force Institute of Technology. He holds a doctorate in Electrical Engineering and has expertise in machine learning, with a focus on its application to cybersecurity and malware detection. He is also the founder of SIMAPTIC and the Director of Security Research at BC Security, where he specializes in adversary tactics and emulation planning, Red and Blue Team operations, and embedded systems security. Dr. Rose is credited with 16 CVEs and has presented at numerous security conferences, including Black Hat, DEF CON, HackSpaceCon, HackMiami, and RSA Conference.

SpeakerBio: Hana Christensen

Hana Christensen is a second lieutenant and developmental engineer (electrical) in the United States Air Force. She is currently pursuing a master's in electrical engineering, with a focus on signal processing and machine learning. Her research investigates security vulnerabilities in AI hardware, examining whether side-channel analysis can be used to extract information about machine learning algorithms. She holds a B.S. in Electrical and Computer Engineering from the United States Air Force Academy (class of 2025).



Social Gatherings/Events - Saturday - 21:00-00:59 PDT

Title: GOTHCON

Tags: Party

When: Saturday, Aug 8, 21:00 - 00:59 PDT

Where: LVCCW Level 1 Hall 3 801 (Creator Stage 2) - [Map](#)

Description:

Returning for their 9th year, Gothcon invites you to come dance the night away with a line-up of some of the community's best dark dance music DJ's from across the US! Dress however you would like in whatever makes you feel comfortable and happy, and all are welcome.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Gotta Catch 'Em All: How To Capture 3.5 Billion WhatsApp Accounts

Tags: DEF CON Official Talk | Exploit

When: Friday, Aug 7, 17:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 3 906 (Main Track 3) - [Map](#)

Description:

Contact discovery on instant messengers is designed to help users find their friends. But when identifiers are predictable and safeguards are weak, it allows attackers to find everyone. At that point, "catching 'em all" stops being a slogan and becomes an engineering problem.

In this talk, we show how we turned WhatsApp into a global Pokédex. By combining reverse-engineered API access with large-scale phone number generation, we probed tens of billions of candidates and identified over 3.5 billion active WhatsApp accounts --- all from a single machine, without raising flags and getting blocked.

Beyond simple presence checks, enumeration exposes rich metadata, including profile pictures, public keys, device information, timestamps, and user-defined about tags. This enables both macroscopic insights into global platform usage and profiling of individual users.

Our analysis uncovers systemic issues, such as persistent exposure of numbers from historical data leaks and reuse of cryptographic keys across accounts. Moreover, we expose signals of criminal activity (e.g., drug dealers and scam factories), and measurable activity in regions where WhatsApp is officially restricted (e.g., North Korea).

At global scale, small design decisions become big problems. This is what allowed us to complete our 3.5B-sized Pokédex.

<https://github.com/sbaresearch/whatsapp-census>

Paper: Hey there! You are using WhatsApp: Enumerating Three Billion Accounts for Security and Privacy, Gegenhuber et al., NDSS 2026

Speakers: Maximilian Guenther, Gabriel Gegenhuber

SpeakerBio: Maximilian Guenther, SBA Research

Max Guenther is master student at University of Vienna. He is a cybersecurity nerd and research engineer at XBow. Previously, he was security analyst at Austrian Power Grid and security researcher at the Austrian Armed Forces.

SpeakerBio: Gabriel Gegenhuber, University of Vienna

Gabriel is working on measuring cellular networks, mobile communication and the Internet. In recent years, his research has examined security and privacy issues in global instant messaging platforms that use end-to-end encryption, such as WhatsApp and Signal. He completed his bachelor's and master's degrees at TU Wien and his PhD at the University of Vienna. He is currently a postdoctoral researcher at IT:U Linz.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Gotta Phish 'Em All! Novel Attack Techniques via Persistent Browser-in-the-Middle

Tags: DEF CON Official Talk | Demo | Tool

When: Sunday, Aug 9, 10:30 - 11:30 PDT

Where: LVCCW Level 1 Hall 3 906 (Main Track 3) - [Map](#)

Description:

Browser-in-the-Middle (BitM) phishing is no longer just a research curiosity. Since its 2021 formalization, BitM has been cataloged by MITRE as an official attack pattern, recognized as a severe threat to MFA-protected web applications. Because the victim authenticates directly through the attacker's browser rather than their own, the technique effectively bypasses most traditional forms of MFA.

This talk presents two years of research on weaponizing BitM for advanced offensive operations. We investigated what novel attack techniques become possible when an attacker fully controls the browser the victim interacts with. This includes real-time keystroke logging, in-transit file interception and silent modification, session persistence that keeps operator access alive long after the victim logs out, and microphone/webcam capture achieved through social-engineered browser flows.

The practical validation of this research is P-BitM, the first open-source framework for Persistent Browser-in-the-Middle spear-phishing, which will be released at DEF CON 34. The "Persistent" in P-BitM carries its full offensive meaning: a single phishing click becomes a persistent beachhead. We will break down our core research, demonstrate these new attack vectors via demo videos, and showcase the capabilities of the tool.

<https://link.springer.com/article/10.1007/s10207-021-00548-5> <https://github.com/JoelGMSec/EvilnoVNC>

<https://github.com/b3rito/peeko>

SpeakerBio: Giacomo "GiaccoLenzo2109" Lenzini, EY

Giacomo Lenzini is an Offensive Security Specialist and Red Teamer at EY Italy, and an independent security researcher. His work focuses on adversary simulation, red team operations, and penetration testing. He has received recognition from organizations such as NASA and has identified several vulnerabilities with associated CVEs.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Governing the Firehose: Writing Custom OPA Policies to Tame and Remediate Prowler Output

Tags: Cloud Village | Creator Event/Activity | Strategic Defense

When: Friday, Aug 7, 11:00 - 12:59 PDT

Where: LVCCW Level 3 W311 (Cloud Village Labs) B - [Map](#)

Description:

When you run an opensource CSPM tool like Prowler across an cloud environment, you don't get an audit; you get a tsunami of raw data. Sifting through thousands of JSON lines to determine what actually poses an active threat to your specific architecture is where most cloud defense pipelines break down.

In this 2-hour hands-on workshop, I'm going to show you how I bridge the gap between scanning and governance using Policy as Code. We will dive straight into treating Prowler's raw security findings as structured data input for Open Policy Agent (OPA).

Together, we'll write custom Rego policies from scratch to parse, filter and logically route Prowler results based on real world business context. I'll show you how to write policies that evaluate infrastructure as code risk, suppress known risk acceptances safely and isolate critical failures (like exposed storage buckets or unencrypted databases) to trigger automated remediation workflows.

SpeakerBio: Ram "n2r"

Passionate about Linux, cryptography, and secure SDLC, I love digging into code, threat modeling, and breaking things (responsibly ofc). Whether it's hardening apps or decoding exploits. I'm all about making software safer - one commit at a time.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: gpwn: Wiretapping fiber (GPON) ISP deployments from the comfort of your home

Tags: DEF CON Official Talk | Demo | Tool | Exploit

When: Saturday, Aug 8, 13:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 3 1006 (Main Track 1) - [Map](#)

Description:

Have you ever wanted to know what your neighbor does on their network and what sites they're browsing? How about all the people around you on their mobile phones, on cellular data?

GPON is the fiber-to-home protocol that carries traffic for hundreds of millions of subscribers worldwide (and climbing). It operates on a threat model that makes several assumptions that break in the real world.

We'll chat about how it's possible to become a modern day fiber optic voyeur with hardware that costs about \$100 and watch your neighbor's DNS, SIP calls and most excitingly, GTP-tunneled 4G/5G traffic from the cellular towers that you share a fiber line with.

Additionally, we show some fun, new techniques to retain your access even if your ISP wisens up and enables downstream AES encryption, by hacking the Optical Line Terminal itself over the fiber line, and how to build your own botnet army out of all the members of your ISP.

Finally, we'll also explore how we built custom hardware to read and write onto a fiber line despite the rules of the network (and land).

- [Anime4000 repo with prior art on modifying the RTL960x family of chipsets](#)
- [GPON FTTH networks \(in\)security](#)
- [Hack GPON community](#)

Speakers: Rithwik "the131" Jayasimha, Rithvik Vibhu

SpeakerBio: Rithwik "the131" Jayasimha, Lagrange Point

Rithwik is a hacker who's been breaking into systems since the impressionable age of 10.

SpeakerBio: Rithvik Vibhu, Lagrange Point

Rithvik has always been fascinated by network systems and in the past was a core contributor to the HNS ecosystem. In the past, he reverse engineered an implementation of UPI in India, and built distributed proxy infra.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Groking the Kill Chain

Tags: Recon Village | Creator Talk/Panel

When: Friday, Aug 7, 16:30 - 16:59 PDT

Where: LVCCW Level 1 Hall 3 1102 (Creator Stage 6) - [Map](#)

Description:

Most LLM-powered recon tools look impressive in a 90-second demo and fall apart on real targets. They hallucinate, loop, go out of scope, double-fire the same endpoint, or die the moment a WAF or rate limit appears. This talk is about what it actually takes to run fifty-plus specialist agents in parallel for hours or days without the chaos.

We built a system where every agent is locked to the rails: a concrete tool, a strict pipeline phase, explicit prerequisites, timeouts, and sandboxes. The model does not drive. It rides. The binaries (and only the binaries) touch the target. This "Agents on Rails" approach eliminates freestyle LLM behavior while still letting the model do what it is good at—reasoning over evidence.

SpeakerBio: Anthony Russell, Cyber Security Software Engineer

Anthony Russell, is a senior cyber security engineer with over 13 years of professional experience building software. He has a focus in information security and has been featured in 2600 magazine, on Hak5 and has spoken at both Defcon and DerbyCon multiple times. Favorite things to discuss are blockchain technology, baking custom IoT devices, and everything infosec. You can see more of Anthony's work at SquidHacker.com or Twitter.com/DotNetRussell

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Contests - Saturday - 10:00-17:59 PDT

Title: Hac-Man

Tags: Hac-Man | Contest

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 213 (Hac-Man (Rogue Signal)) - [Map](#)

Description:

Rogue Signal builds bespoke, technically driven interactive experiences rooted in hacker culture, game design, and immersive storytelling. Drawing from backgrounds in immersive theater, live events production, community building, and deep game design practice, Rogue Signal creates systems that transform participation into exploration.

Rather than relying on superficial gamification, Rogue Signal focuses on meaningful challenge design. Their experiences reward curiosity, experimentation, collaboration, and strategic thinking. From scavenger hunts to technical skill challenges to digital easter eggs, each activation is designed around the specific audience and environment it lives in.

At DEF CON, Rogue Signal brings that philosophy to Hac-Man. A Pac-Man-themed security challenge platform that blends retro inspiration with layered technical depth. Participants will engage directly with structured challenges that test logic, pattern recognition, foundational security and hacker knowledge, and progressively more advanced technical skills.

Hac-Man reflects the hacker mindset: iterate, experiment, fail, refine, break assumptions, and try again. It encourages collaboration where helpful, competition where motivating, and discovery at every level.

Attendees can expect: - Hands-on security challenges - Multiple subject-matter tracks - Layered difficulty levels - Scavenger style discovery elements - Competitive scoring and mission style progression - A welcoming but technically rich environment

Whether you're new to security or already deep in the field, Rogue Signal's space offers a place to test your thinking, sharpen your skills, and experience hacking concepts through play.

Participant Prerequisites

Participants will need access to a smartphone, tablet, or laptop in order to access gameplay content and view leaderboards. The experience is web-accessible and designed to function on standard modern devices.

No specialized hardware (e.g., Flipper Zero, SDR, etc.) is required. Foundational familiarity with basic computer use and logical problem-solving will be helpful, but no advanced security knowledge is required to begin. The game features layered difficulty tracks to accommodate both beginners and more advanced participants.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Hac-Man

Tags: Hac-Man | Contest

When: Sunday, Aug 9, 10:00 - 11:59 PDT

Where: LVCCW Level 1 Hall 1 213 (Hac-Man (Rogue Signal)) - [Map](#)

Description:

Rogue Signal builds bespoke, technically driven interactive experiences rooted in hacker culture, game design, and immersive storytelling. Drawing from backgrounds in immersive theater, live events production, community building, and deep game design practice, Rogue Signal creates systems that transform participation into exploration.

Rather than relying on superficial gamification, Rogue Signal focuses on meaningful challenge design. Their experiences reward curiosity, experimentation, collaboration, and strategic thinking. From scavenger hunts to technical skill challenges to digital easter eggs, each activation is designed around the specific audience and environment it lives in.

At DEF CON, Rogue Signal brings that philosophy to Hac-Man. A Pac-Man-themed security challenge platform that blends retro inspiration with layered technical depth. Participants will engage directly with structured challenges that test logic, pattern recognition, foundational security and hacker knowledge, and progressively more advanced technical skills.

Hac-Man reflects the hacker mindset: iterate, experiment, fail, refine, break assumptions, and try again. It encourages collaboration where helpful, competition where motivating, and discovery at every level.

Attendees can expect: - Hands-on security challenges - Multiple subject-matter tracks - Layered difficulty levels - Scavenger style discovery elements - Competitive scoring and mission style progression - A welcoming but technically rich environment

Whether you're new to security or already deep in the field, Rogue Signal's space offers a place to test your thinking, sharpen your skills, and experience hacking concepts through play.

Participant Prerequisites

Participants will need access to a smartphone, tablet, or laptop in order to access gameplay content and view leaderboards. The experience is web-accessible and designed to function on standard modern devices.

No specialized hardware (e.g., Flipper Zero, SDR, etc.) is required. Foundational familiarity with basic computer use and logical problem-solving will be helpful, but no advanced security knowledge is required to begin. The game features layered difficulty tracks to accommodate both beginners and more advanced participants.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Hac-Man

Tags: Hac-Man | Contest

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 213 (Hac-Man (Rogue Signal)) - [Map](#)

Description:

Rogue Signal builds bespoke, technically driven interactive experiences rooted in hacker culture, game design, and immersive storytelling. Drawing from backgrounds in immersive theater, live events production, community building, and deep game design practice, Rogue Signal creates systems that transform participation into exploration.

Rather than relying on superficial gamification, Rogue Signal focuses on meaningful challenge design. Their experiences reward curiosity, experimentation, collaboration, and strategic thinking. From scavenger hunts to technical skill challenges to digital easter eggs, each activation is designed around the specific audience and environment it lives in.

At DEF CON, Rogue Signal brings that philosophy to Hac-Man. A Pac-Man-themed security challenge platform that blends retro inspiration with layered technical depth. Participants will engage directly with structured challenges that test logic, pattern recognition, foundational security and hacker knowledge, and progressively more advanced technical skills.

Hac-Man reflects the hacker mindset: iterate, experiment, fail, refine, break assumptions, and try again. It encourages collaboration where helpful, competition where motivating, and discovery at every level.

Attendees can expect: - Hands-on security challenges - Multiple subject-matter tracks - Layered difficulty levels - Scavenger style discovery elements - Competitive scoring and mission style progression - A welcoming but technically rich environment

Whether you're new to security or already deep in the field, Rogue Signal's space offers a place to test your thinking, sharpen your skills, and experience hacking concepts through play.

Participant Prerequisites

Participants will need access to a smartphone, tablet, or laptop in order to access gameplay content and view leaderboards. The experience is web-accessible and designed to function on standard modern devices.

No specialized hardware (e.g., Flipper Zero, SDR, etc.) is required. Foundational familiarity with basic computer use and logical problem-solving will be helpful, but no advanced security knowledge is required to begin. The game features layered difficulty tracks to accommodate both beginners and more advanced participants.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Hack the Airwaves – Embedded Wireless for Next-Gen Hackers

Tags: DCNextGen | Creator Talk/Panel | Youth

When: Friday, Aug 7, 14:00 - 14:45 PDT

Where: LVCCW Level 3 W316 (DC NextGen) - [Map](#)

Description:

Win an AWOK Dual C5 just by showing up! Join Adventures of Illya for Hack the Airwaves! Explore wireless technology with live demos featuring the AWOK Dual C5, ByteShield, H4M PortaPack, Flipper Zero, ESP32 boards, LoRa, RFID, NFC, and CC1101. Learn how these technologies work, ask questions, and get inspired to build your own projects.

SpeakerBio: Adventures of Illya

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Noob Community - Friday - 10:00-17:59 PDT

Title: Hack The Box DC Junior Ranger Program Challenge

Tags: Noob Community | Creator Event/Activity

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 4 1417 (Noob Community) - [Map](#)

Description:

Hack The Box brings its Junior Ranger Program to DEF CON: a beginner-friendly challenge guide built by the Hack The Box team specifically for the Noob Village, modeled after the U.S. National Park Service's Junior Ranger booklets. Work through the challenges in the guide and earn custom Junior Ranger badges as you complete them. Hack The Box is the leading cyber readiness platform for the agentic era, battle-testing and upskilling both humans and AI agents to enhance organizational cyber resilience.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Noob Community - Saturday - 10:00-17:59 PDT

Title: Hack The Box DC Junior Ranger Program Challenge

Tags: Noob Community | Creator Event/Activity

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 4 1417 (Noob Community) - [Map](#)

Description:

Hack The Box brings its Junior Ranger Program to DEF CON: a beginner-friendly challenge guide built by the Hack The Box team specifically for the Noob Village, modeled after the U.S. National Park Service's Junior Ranger booklets. Work through the challenges in the guide and earn custom Junior Ranger badges as you complete them. Hack The Box is the leading cyber readiness platform for the agentic era, battle-testing and upskilling both humans and AI agents to enhance organizational cyber resilience.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Noob Community - Sunday - 10:00-13:59 PDT

Title: Hack The Box DC Junior Ranger Program Challenge

Tags: Noob Community | Creator Event/Activity

When: Sunday, Aug 9, 10:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 4 1417 (Noob Community) - [Map](#)

Description:

Hack The Box brings its Junior Ranger Program to DEF CON: a beginner-friendly challenge guide built by the Hack The Box team specifically for the Noob Village, modeled after the U.S. National Park Service's Junior Ranger booklets. Work through the challenges in the guide and earn custom Junior Ranger badges as you complete them. Hack The Box is the leading cyber readiness platform for the agentic era, battle-testing and upskilling both humans and AI agents to enhance organizational cyber resilience.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Hack the Duck Store

Tags: AppSec Village | Creator Event/Activity || All Audiences

When: Friday, Aug 7, 11:00 - 12:59 PDT

Where: LVCCW Level 1 Hall 2 604 (Appsec Village) POD 4 - [Map](#)

Description:

At a developer meetup on secure software development, we asked a simple question: look at this login form, how could a hacker abuse it? Not one developer in the room dared to answer. The referral code field looked harmless. The backend had no validation: self-referrals, circular referrals, unlimited farming - all possible. It's just the simplest example of how business logic flaws get missed. This card game is built around that gap, showing what business logic vulnerabilities might exist and how the real vulnerabilities, hiding inside the intentionally vulnerable app, Duck Store, can be abused.

Speakers: Gwendal Mognier, Samantha Pearlstein

SpeakerBio: Gwendal Mognier

Gwendal Mognier is a Security Researcher at Escape. He's passionate about cybersecurity and always eager to learn new ways to break and secure systems. Gwendal is focused on discovering vulnerabilities and helping improve security across the board.

SpeakerBio: Samantha Pearlstein, Founding Solutions Engineer at Escape

Samantha is a solutions engineer with a strong background in security research, executive cyber resilience, and nation-state threats. As a former consultant at Accenture, she led cyber resilience initiatives for Fortune 100 executives, developed GenAI-powered security tools, and delivered workshops on emerging cyber challenges. Today, as a Sales Engineer at Escape, Samantha helps AppSec teams secure their APIs and SPAs, combining her passion for cybersecurity with hands-on problem-solving.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Hack the Planet (not ours)

Tags: Radio Frequency Village | Creator Talk/Panel

When: Friday, Aug 7, 15:00 - 15:25 PDT

Where: LVCCW Level 1 Hall 1 409 (Radio Frequency Village) - [Map](#)

Description:

What does it take to bounce a signal off Venus and hear it back on Earth? Quite a lot, actually. And we're going to show all of it to you.

In 2008, AMSAT-DL aimed a carrier wave from a dangerously powerful magnetron-based transmitter, located at the Bochum Observatory, at Venus. Four minutes later, they heard an echo. This was the first time amateurs had bounced a signal of any type off of another planet. This is a significant and enduring achievement.

However, a radar signal has no information in it. It's a dead carrier. What does it take to bounce a communications signal off of Venus, and hear it back here on Earth? First of all, the path loss is immense. Then, Venus only returns about 13% of the signal that hits it. And, it's spinning. Information in a signal requires more signal to noise ratio when compared to a dead carrier, and reflecting off a spinning surface damages information signals in particular ways that stationary reflectors do not.

Venus and Earth encounter each other in their orbits only once every 18 months or so. This is the inferior conjunction of the two planets. Unlike the Moon, frequently used by radio enthusiasts as a reflector, Venus is barely close enough every 18 months for the largest amateur and citizen science dishes to reach. This makes timing, preparation, and coordination equally as important as resolving the technical challenges.

What are the different parts of an Earth-Venus-Earth digital communications system? Which parts make the most difference? What needed to be developed? How did coordination go? What will happen next? Come to the talk and find out how we are going to Hack a Planet.

Quite a lot, actually. And we're going to show all of it to you.

SpeakerBio: Abraxas3d, CEO ORI

Michelle Thompson, W5NYV, is the CEO of Open Research Institute, a 501(c)(3) nonprofit developing open source digital radio and space communication systems. ORI's work directly benefits the amateur radio and amateur radio satellite services. She served as IEEE San Diego Section Chair and represents ORI on the FCC Technological Advisory Council, including co-chairing the AI/ML Safe Uses Sub-Working Group. Her technical background spans RF engineering, digital signal processing, FPGA development, and satellite communications, with prior industry experience at Qualcomm, Smithville Telephone, and Apiary. She can be reached at w5nyv@arrl.net.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Contests - Saturday - 10:00-11:59 PDT

Title: Hack3r Runw@y v8.0

Tags: Hack3r Runw@y v8.0 | Contest

When: Saturday, Aug 8, 10:00 - 11:59 PDT

Where: LVCCW Level 1 Hall 1 100 (Contest Stage) - [Map](#)

Description:

Hack3r Runw@y v8.0

Where Code Meets Catwalk @ DEF CON 34

The Hack3r Runw@y returns for its 8th evolution! After nearly a decade of bridging the gap between hardware and haberdashery, we're back at DEF CON 34 to prove once again that hackers are the most creative engineers on the planet.

Whether you're a glamorous geek, a crafty coder, or a fashionably functional phantom, it's time to weaponize your wardrobe. We're challenging you to dismantle the boundary between "security" and "style." If you can hack it, you can wear it.

The Mission Categories - Smart-Wear (Active Tech): The high-voltage category. Integrate microcontrollers, sensors, and live telemetry into your designs. We want to see hardware that reacts to the environment—or the wearer—in real-time. - Digital Dazzle (Passive Tech): Bling with a brain. Focus on LEDs, fiber optics, and glow-tech that remains passive but high-impact. Light up the room without needing a CLI. - Functional Fashion (Tactical): Gear for the field. Think "Cyber-Chic Pentester": lockpick jewelry, shim-integrated accessories, signal-blocking fabrics, or high-fashion physical security tools. - Extraordinary Style (Creative Ops): The "Kitbash" category. Elevate the everyday with 3D textures, optical illusions, security-inspired patterns, and deep-cut cosplay.

THE PEOPLE'S CHOICE Trophy: One coveted trophy is up for grabs where ANYONE can win. But be warned: in true DEF CON fashion, there will be a twist. Follow the social media for updates.

- The Maker's Mandate
- This is a pure DIY challenge. We value the "Proof of Concept" over the "Price Tag."
- Originality is King: Items must be handmade or heavily modified ("kitbashed") by the entrant.
- No "Off-the-Shelf": Integrating components (like an Arduino or LED strip) is encouraged; buying a pre-finished "light-up dress" from a mass-retailer is an automatic DQ.
- Show Your Work: Documentation is required. Have photos, videos, or a build-log ready to prove your process if the judges need to verify your "hacker's trail."

The Judging Criteria

Our panel will be scoring builds based on: - Technical Mastery: Execution of hardware/software. - Couture Craftsmanship: Quality of the "fit" and finish. - Relevance: How it speaks to hacker culture or security. - Originality: Creative use of materials and "kitbashing."

Participant Prerequisites

Originality: Items must be handmade by the entrant.

Verification: Documentation (photos/video) of the build process is required to verify authenticity.

Modification vs. Acquisition: We celebrate the "kitbash." Using pre-made components to create something new is allowed, but "off-the-shelf" or "plug-and-play" retail items are not permitted.



Title: Hackbots

Tags: Bug Bounty Village | Creator Talk/Panel

When: Friday, Aug 7, 11:30 - 12:30 PDT

Where: LVCCW Level 2 W206-207 (Bug Bounty Village) - [Map](#)

Description:

Building AI-Powered Penetration Testing Bots

In this talk, we'll walk through the core design philosophy behind AI hackbots and the architecture that makes them work: single-purpose vs. multi-stage bots, context engineering for targeted prompting, and tool integration with output parsing workflows.

Then we'll get hands-on. We'll live-build a functional hackbot for a common offensive task —demonstrating asset discovery, endpoint analysis, or mutation-focused testing (e.g., XSS/SSRF) — and show how context engineering and hallucination mitigation work in practice against real targets. You'll see where AI genuinely accelerates reconnaissance and web analysis, and where it falls flat if you aren't careful. We'll close with lessons on cost optimization, auditability, and integrating hackbots into actual engagements.

Who should attend: Pentesters and bug bounty hunters with offensive security experience who want to meaningfully integrate AI into their workflow — not as a novelty, but as reliable tooling.

What you'll walk away with: A clear mental model for when and how to build hackbots, a live demo you can replicate, and a path into the full course where you'll build seven production-ready bots from asset discovery through mutation testing.

Speakers: Jason "jhaddix" Haddix, Ryan "BadAt_Computers" Bonner

SpeakerBio: Jason "jhaddix" Haddix, CEO and "Hacker in Charge" at Arcanum Information Security

Jason Haddix AKA jhaddix is the CEO and “Hacker in Charge” at Arcanum Information Security. Arcanum is a world class assessment and training company.

Jason has had a distinguished 20-year career in cybersecurity previously serving as CISO of FLARE, CISO of Buddobot, CISO of Ubisoft, Head of Trust/Security/Operations at Bugcrowd, Director of Penetration Testing at HP, and Lead Penetration Tester at Redspin. He has also held positions doing mobile penetration testing, network/infrastructure security assessments, and static analysis. Jason is a hacker, bug hunter and currently ranked 57th all-time on Bugcrowd’s bug bounty leaderboards. Currently, he specializes in recon, web application analysis, and emerging technologies. Jason has also authored many talks on offensive security methodology, including speaking at cons such as DEFCON, Bsides, BlackHat, RSA, OWASP, Nullcon, SANS, IANS, BruCon, Toorcon and many more.

SpeakerBio: Ryan "BadAt_Computers" Bonner, Lead Security Engineer, Arcanum Information Security

Ryan is a Lead Security Engineer at Arcanum Information Security. A part-time bug hunter, Ryan has built his career on the offensive side of security, focusing on where AI systems and integrations meet the modern web. He specializes in attacking AI-powered applications, including prompt injection, agent, and integration weaknesses that appear as large language models get wired into real products.



Social Gatherings/Events - Friday - 14:00-15:59 PDT

Title: Hacker Book Club Discussion

Tags: Meetup

When: Friday, Aug 7, 14:00 - 15:59 PDT

Where: LVCCW Level 3 W301 (Misc Meeting Room) - [Map](#)

Description:

Community is essential and so is continual learning. Reading books and discussing books can greatly impact an individual's access and sense of community and knowledge. This Hacker Book Club book discussion will be an accessible group aiming to build community and share out learnings, all in a quieter setting. Come join us and discuss what you've been reading. We also run a year round Discord to discuss books throughout the year, hackerbookclub.com. This Hacker Book Club is not locked to a region and is for those who love books and escaping to the cyperpunk, scifi worlds that inspire DEF CON and modern literature.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

The Diana Initiative - Saturday - 14:00-15:59 PDT

Title: Hacker Book Club meet up

Tags: The Diana Initiative | Creator Event/Activity

When: Saturday, Aug 8, 14:00 - 15:59 PDT

Where: LVCCW Level 2 W209 (Diana Initiative) - [Map](#)

Description:

Community is essential and so is continual learning. Reading books and discussing books can greatly impact an individual's access and sense of community and knowledge. This Hacker Book Club book discussion will be an accessible group aiming to build community and share out learnings, all in a quieter setting. Come join us and discuss what you've been reading. We also run a year round Discord to discuss books throughout the year, hackerbookclub.com. This Hacker Book Club is not locked to a region and is for those who love books and escaping to the cyberpunk and scifi worlds that inspire DEF CON and modern literature. The DEF CON 34 theme is agency and our DEF CON themed book is *The Dispossessed* by Ursula Le Guin.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Hacker Culture 101

Tags: DCNextGen | Creator Event/Activity | Youth

When: Saturday, Aug 8, 13:00 - 14:15 PDT

Where: LVCCW Level 3 W316 (DC NextGen) - [Map](#)

Description:

Learn about the K-Rad side of hacking, from media representations in movies and tv shows, to hacker fashion throughout the years (we wear more than black hoodies!). In this session, we will also cover two iconic pieces of hacker culture- Handles and stickers, with an opportunity to make your own stickers and choose your unique handle! If you wanna jam with the console cowboys in cyberspace, this is the event for you!

SpeakerBio: medus4

No BIO available

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Contests - Saturday - 10:00-17:59 PDT

Title: Hacker Games

Tags: Hacker Games | Contest

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 207 (Hacker Games) - [Map](#)

Description:

The Hacker Games is a series of hacker skills tests meant to challenge the hacker's knowledge of computer systems such as Binary -> Hex -> X conversion, Adapter -> Adapter knowledge, Keyboard Layout, and many more arbitrarily useless skills. Hackers will go head-to-head in a series of several skill-based games. BinHexAscii, Chopstick Challenge (a.k.a. Will it Flow), Keyboard Layout, Adapt or Die, ToS, and more! Can you hack it?

Participant Prerequisites

A box of computer-style adapters of no particular order would be very helpful.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Contests - Sunday - 10:00-11:59 PDT

Title: Hacker Games

Tags: Hacker Games | Contest

When: Sunday, Aug 9, 10:00 - 11:59 PDT

Where: LVCCW Level 1 Hall 1 207 (Hacker Games) - [Map](#)

Description:

The Hacker Games is a series of hacker skills tests meant to challenge the hacker's knowledge of computer systems such as Binary -> Hex -> X conversion, Adapter -> Adapter knowledge, Keyboard Layout, and many more arbitrarily useless skills. Hackers will go head-to-head in a series of several skill-based games. BinHexAscii, Chopstick Challenge (a.k.a. Will it Flow), Keyboard Layout, Adapt or Die, ToS, and more! Can you hack it?

Participant Prerequisites

A box of computer-style adapters of no particular order would be very helpful.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Contests - Friday - 10:00-17:59 PDT

Title: Hacker Games

Tags: Hacker Games | Contest

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 207 (Hacker Games) - [Map](#)

Description:

The Hacker Games is a series of hacker skills tests meant to challenge the hacker's knowledge of computer systems such as Binary -> Hex -> X conversion, Adapter -> Adapter knowledge, Keyboard Layout, and many more arbitrarily useless skills. Hackers will go head-to-head in a series of several skill-based games. BinHexAscii, Chopstick Challenge (a.k.a. Will it Flow), Keyboard Layout, Adapt or Die, ToS, and more! Can you hack it?

Participant Prerequisites

A box of computer-style adapters of no particular order would be very helpful.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Social Gatherings/Events - Saturday - 20:00-21:59 PDT

Title: Hacker Jeopardy

Tags: Event | Hacker Jeopardy!

When: Saturday, Aug 8, 20:00 - 21:59 PDT

Where: LVCCW Level 1 Hall 3 1006,904 (Main Tracks 1,4) - [Map](#)

Description:



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Social Gatherings/Events - Friday - 20:00-21:59 PDT

Title: Hacker Jeopardy

Tags: Event | Hacker Jeopardy!

When: Friday, Aug 7, 20:00 - 21:59 PDT

Where: LVCCW Level 1 Hall 3 1006,904 (Main Tracks 1,4) - [Map](#)

Description:



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Social Gatherings/Events - Friday - 20:00-00:59 PDT

Title: Hacker Karaoke

Tags: Party

When: Friday, Aug 7, 20:00 - 00:59 PDT

Where: LVCCW Level 2 W229, W232 - [Map](#)

Description:

Two great things that go great together! Join the fun as your fellow hackers make their way through songs from every era and style. Everyone has a voice and this is your opportunity to show it off! Everyone is encourage to participate in a DEF CON tradition from all folks and skill levels.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Social Gatherings/Events - Saturday - 20:00-00:59 PDT

Title: Hacker Karaoke

Tags: Party

When: Saturday, Aug 8, 20:00 - 00:59 PDT

Where: LVCCW Level 2 W229, W232 - [Map](#)

Description:

Two great things that go great together! Join the fun as your fellow hackers make their way through songs from every era and style. Everyone has a voice and this is your opportunity to show it off! Everyone is encourage to participate in a DEF CON tradition from all folks and skill levels.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

The Diana Initiative - Friday - 10:00-11:59 PDT

Title: Hacker Runway Crafting Time

Tags: The Diana Initiative | Hack3r Runw@y v8.0 | Creator Event/Activity

When: Friday, Aug 7, 10:00 - 11:59 PDT

Where: LVCCW Level 2 W209 (Diana Initiative) - [Map](#)

Description:

Hacker Runway Crafting time - didn't have time, or didn't know about the Hacker Runway competition? Have no fear we have some supplies to help you put together a last moment entry! Make sure to stop by the DC Maker Village as well!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Hackers.town - Friday - 16:00-16:59 PDT

Title: Hackers Trivia

Tags: Hackers.town | Creator Talk/Panel

When: Friday, Aug 7, 16:00 - 16:59 PDT

Where: LVCCW Level 1 Hall 4 1420 (Hackers.town) - [Map](#)

Description:

Speakers: RemoteNemesis, Medus4

SpeakerBio: RemoteNemesis

No BIO available

SpeakerBio: Medus4

No BIO available

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

The Diana Initiative - Saturday - 13:20-13:30 PDT

Title: Hackers with Disabilities Tour

Tags: The Diana Initiative | Creator Tour

When: Saturday, Aug 8, 13:20 - 13:30 PDT

Where: LVCCW Level 1 South Lobby / Atrium - [Map](#)

Description:

Interested in visiting Hackers with Disabilities but afraid to go by yourself? The Diana Initiative is hosting tours! Follow a volunteer to Hackers with Disabilities and be introduced to the community and activities inside!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Contests - Sunday - 10:00-11:59 PDT

Title: HackFortress

Tags: HackFortress | Contest

When: Sunday, Aug 9, 10:00 - 11:59 PDT

Where: LVCCW Level 1 Hall 1 108 (HackFortress) - [Map](#)

Description:

HackFortress is back! Returning to DEF CON with a twist on our standard format. Two teams of players, 6 gamers and 4 hackers each, compete in a mashup of a jeopardy style CTF and a first person shooter. New this year, we're replacing our previous FPS of Team Fortress 2 with a web based version of the 2000's classic Quake 3!

While gamers are rocket jumping and sniping each other in Quake, hackers will be solving challenges in a variety of areas: web security, network security, cryptography, lock picking, social engineering, and more! Challenges range from beginner to advanced, from serious to absurd. During the competition, as both sides of the team star scoring points, the teams also earn points in the HackFortress HackConomy Store, in the store hackers can buy in game effects, both offensive and defensive, and much like the challenges, these effects range from serious to absurd.

With all of the contest being web based, both hacking and Quake, players **MUST** bring their own laptop (or whatever device they want to use) and a wired network adapter.

Grab your friends!

Ask that random stranger standing next to you in Linecon if they want to join your team!

Come play HACKFORTRESS!

Participant Prerequisites

All players will need to bring a laptop and wired network adapter. Since we are now using web based version of Quake 3 (which can run on players phones), we are no longer providing any gaming laptops.

Gamers: bring any gaming accessory of your choice, its your hardware, go for it

Hackers: bring lockpicks

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Contests - Friday - 10:00-17:59 PDT

Title: HackFortress

Tags: HackFortress | Contest

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 108 (HackFortress) - [Map](#)

Description:

HackFortress is back! Returning to DEF CON with a twist on our standard format. Two teams of players, 6 gamers and 4 hackers each, compete in a mashup of a jeopardy style CTF and a first person shooter. New this year, we're replacing our previous FPS of Team Fortress 2 with a web based version of the 2000's classic Quake 3!

While gamers are rocket jumping and sniping each other in Quake, hackers will be solving challenges in a variety of areas: web security, network security, cryptography, lock picking, social engineering, and more! Challenges range from beginner to advanced, from serious to absurd. During the competition, as both sides of the team star scoring points, the teams also earn points in the HackFortress HackConomy Store, in the store hackers can buy in game effects, both offensive and defensive, and much like the challenges, these effects range from serious to absurd.

With all of the contest being web based, both hacking and Quake, players **MUST** bring their own laptop (or whatever device they want to use) and a wired network adapter.

Grab your friends!

Ask that random stranger standing next to you in Linecon if they want to join your team!

Come play HACKFORTRESS!

Participant Prerequisites

All players will need to bring a laptop and wired network adapter. Since we are now using web based version of Quake 3 (which can run on players phones), we are no longer providing any gaming laptops.

Gamers: bring any gaming accessory of your choice, its your hardware, go for it

Hackers: bring lockpicks

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Contests - Saturday - 10:00-17:59 PDT

Title: HackFortress

Tags: HackFortress | Contest

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 108 (HackFortress) - [Map](#)

Description:

HackFortress is back! Returning to DEF CON with a twist on our standard format. Two teams of players, 6 gamers and 4 hackers each, compete in a mashup of a jeopardy style CTF and a first person shooter. New this year, we're replacing our previous FPS of Team Fortress 2 with a web based version of the 2000's classic Quake 3!

While gamers are rocket jumping and sniping each other in Quake, hackers will be solving challenges in a variety of areas: web security, network security, cryptography, lock picking, social engineering, and more! Challenges range from beginner to advanced, from serious to absurd. During the competition, as both sides of the team star scoring points, the teams also earn points in the HackFortress HackConomy Store, in the store hackers can buy in game effects, both offensive and defensive, and much like the challenges, these effects range from serious to absurd.

With all of the contest being web based, both hacking and Quake, players **MUST** bring their own laptop (or whatever device they want to use) and a wired network adapter.

Grab your friends!

Ask that random stranger standing next to you in Linecon if they want to join your team!

Come play HACKFORTRESS!

Participant Prerequisites

All players will need to bring a laptop and wired network adapter. Since we are now using web based version of Quake 3 (which can run on players phones), we are no longer providing any gaming laptops.

Gamers: bring any gaming accessory of your choice, its your hardware, go for it

Hackers: bring lockpicks

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Hacking AFDX or Not; A Primer for Flight Control Systems Security

Tags: Aerospace Village | Creator Talk/Panel

When: Saturday, Aug 8, 14:30 - 14:59 PDT

Where: LVCCW Level 1 Hall 3 1103 (Creator Stage 5) - [Map](#)

Description:

One of the challenges of independent airplane cyber research is the lack of availability of recent hardware; avionics, LRUs and anything from the aircraft control domain is insanely expensive, even when used. Access to retired airframes therefore represents the state of the art from 20+ years ago. We have been stuck with researching older ACD protocols such as ARINC 429 and 629. However, through a fortuitous stroke of luck, we were given access to an ARINC 664 or 'AFDX' environment on a test bench recently. The protocol was developed by Airbus for the A380, but is also found on the B787, A350 and is increasingly being implemented on new designs. Avionics Full-Duplex Switched Ethernet / ADFX will be much more familiar to IT folks than the earlier protocols, having much more in common with the OSI reference model. But, it has crucial differences which requires a steep learning curve. This talk is a primer for interfacing with AFDX and the various security and safety features that it offers.

Speakers: Andrew Tierney, Adam Bromiley

SpeakerBio: Andrew Tierney

No BIO available

SpeakerBio: Adam Bromiley, Pen Test Partners

Adam is a security consultant at Pen Test Partners who specialises in industrial control systems and embedded hardware security. He's worked on everything safety-critical: from high-speed rail to aircraft, power stations, and gas distribution. His embedded work has seen him break driverless cars, slot machines, and drones and has led to the responsible

disclosure of numerous vulnerabilities in industrial controllers. Adam enjoys hands-on and boots-on-the-ground testing, reverse engineering, and providing practical security advice for complex real-world systems.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Hacking AI

Tags: DEF CON Official Talk

When: Friday, Aug 7, 17:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 3 1006 (Main Track 1) - [Map](#)

Description:

Humans are hacking AI systems. Humans are hacking with AI systems. But also, AIs are hacking human systems. They're finding and exploiting vulnerabilities in computer code, and they'll soon be doing the same with all sorts of other codes. For example: the tax code can be hacked. Vulnerabilities are called loopholes, exploits are called tax avoidance strategies, and black hats are called accountants. Similarly, financial markets can be hacked. So can any system of rules or laws, including democracy itself. AIs will hack these systems at our request, and they'll also do this innately, organically – and possibly in ways we don't immediately see. We need to consider a world where increasingly sophisticated hacks on our social, economic, and political systems are discovered at computer speeds, and then exploited at computer scale and scope. Right now, our systems of patching these systems operate at a human pace, which won't be good enough.

<https://www.schneier.com/academic/archives/2021/04/the-coming-ai-hackers.html>

SpeakerBio: Bruce Schneier, Advisory Board Member at VerifiedVoting.org

Bruce Schneier is an internationally renowned security technologist, called a “security guru” by the Economist. He is the New York Times best-selling author of 14 books – including *Rewiring Democracy* and *A Hacker's Mind* -- as well as hundreds of articles, essays, and academic papers. His long-running newsletter and blog, “Schneier on Security,” is one of the most popular sources of cybersecurity news on the internet. Schneier is a Fellow and Lecturer in Public Policy at the Harvard Kennedy School and the Munk School at the University of Toronto. He is a fellow at the Berkman-Klein Center for Internet and Society at Harvard University, a board member of the Electronic Frontier Foundation and AccessNow, and an advisory board member of EPIC and VerifiedVoting.org. He is also the Chief of Security Architecture at Inrupt, Inc.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Aerospace Village - Friday - 13:30-13:59 PDT

Title: Hacking Airplanes at the NTSB

Tags: Aerospace Village | Creator Talk/Panel

When: Friday, Aug 7, 13:30 - 13:59 PDT

Where: LVCCW Level 1 Hall 3 1103 (Creator Stage 5) - [Map](#)

Description:

NTSB Vehicle Recorder Specialists Jonathan Xue and David Case will give a talk on decoding data recovered from several aircraft accidents, and a tourist submarine raised from the depths of the North Atlantic. The NTSB's process for getting data out of broken and damaged equipment will be shown, including searching through gigabytes of random data to find a log, and then converting that data to something human readable. Jonathan and David specialize in converting undocumented binary data recovered from accidents into graphs and charts usable in investigation. Quite often, they are the first people to see what actually happened in an accident.

Speakers:David Case,Jonathan Xue

SpeakerBio: David Case, NTSB

No BIO available

SpeakerBio: Jonathan Xue, NTSB

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

DEF CON Training - Tuesday - 08:30-17:30 PDT

Title: Hacking Android and IOT Apps by Example

Tags: DEF CON Training (Paid) (2-day) | DEF CON Training

When: Tuesday, Aug 11, 08:30 - 17:30 PDT

Where: LVCCW Level 3 W321 (Telecom Village) - [Map](#)

Description:

Speakers: Abraham Aranguren, Abhishek J M, Anirudh Anand

SpeakerBio: Abraham Aranguren

No BIO available

SpeakerBio: Abhishek J M

No BIO available

SpeakerBio: Anirudh Anand

No BIO available

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

DEF CON Training - Monday - 08:30-17:30 PDT

Title: Hacking Android and IOT Apps by Example

Tags: DEF CON Training (Paid) (2-day) | DEF CON Training

When: Monday, Aug 10, 08:30 - 17:30 PDT

Where: LVCCW Level 3 W321 (Telecom Village) - [Map](#)

Description:

Speakers: Abraham Aranguren, Abhishek J M, Anirudh Anand

SpeakerBio: Abraham Aranguren

No BIO available

SpeakerBio: Abhishek J M

No BIO available

SpeakerBio: Anirudh Anand

No BIO available

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Hacking Android Apps in a Structured Way

Tags: Mobile Hacking Community | Creator Event/Activity

When: Friday, Aug 7, 13:00 - 14:30 PDT

Where: LVCCW Level 1 Hall 4 1422 (Mobile Hacking Community) - [Map](#)

Description:

Mobile app testing has many pitfalls and a structured approach is needed to get a holistic picture of the attack surface. The OWASP Mobile Application Security (MAS) project is able to support you with that. In this workshop, you'll get a practical introduction to the MAS ecosystem which consists of the standard, mobile weaknesses and how to test them. You will experience test cases and demos for Android in action for static and dynamic analysis, and learn how to perform a mobile penetration test.

By the end of the workshop, attendees will be able to: - Navigate the OWASP Mobile Application Security (MAS) project (MASVS, MASWE, MASTG) and locate relevant test cases for their own engagements. - Apply a mix of static and dynamic analysis techniques against real Android apps. - Use the right tooling (e.g. frida, semgrep, APKLeaks, jadx, AI-assisted reverse engineering) in their pentest workflow.

Instructions: <https://github.com/sushi2k/defcon34-android-workshop>

Prerequisites: a laptop with 10 GB free disk space; GitHub account and git installed.

SpeakerBio: Sven Schleier, Co-Founder at Bai7 GmbH

Sven has been involved with the Open Worldwide Application Security Project (OWASP) since 2016. As a co-project lead and author, he has made significant contributions to the OWASP MAS (Mobile Application Security) project, which is considered the industry standard for mobile application security, see <https://mas.owasp.org>.

Sven is a frequent speaker and trainer around the world. His audiences range from software developers to students and penetration testers. His engagements often take him to conferences, forums and educational institutions, where he shares his extensive knowledge and insights on mobile and application security.

--

Sven is a co-founder of Bai7 GmbH in Austria, which is specialized in trainings and advisory. He has expertise in cloud security, offensive security engagements (Penetration Testing) and Application Security, notably in guiding software development teams across Mobile and Web Applications throughout the Software Development Life Cycle (SDLC) to integrate robust security measures in from the start.

Besides his day job, Sven is involved with the Open Worldwide Application Security Project (OWASP) since 2016. As a co-project leader and author, he has significantly contributed to the OWASP Mobile Application Security Testing Guide (MASTG) and the OWASP Mobile Application Security Verification Standard (MASVS).

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

DEF CON Training - Monday - 08:30-17:30 PDT

Title: Hacking Cryptography

Tags: DEF CON Training (Paid) (2-day) | DEF CON Training

When: Monday, Aug 10, 08:30 - 17:30 PDT

Where: LVCCW Level 3 W316 (DC NextGen) - [Map](#)

Description:

Speakers: Ruben Gonzalez, Aaron Kaiser

SpeakerBio: Ruben Gonzalez, Neodyme

Crypto PhD, Security Researcher and Trainer at Neodyme

SpeakerBio: Aaron Kaiser

No BIO available

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

DEF CON Training - Tuesday - 08:30-17:30 PDT

Title: Hacking Cryptography

Tags: DEF CON Training (Paid) (2-day) | DEF CON Training

When: Tuesday, Aug 11, 08:30 - 17:30 PDT

Where: LVCCW Level 3 W316 (DC NextGen) - [Map](#)

Description:

Speakers: Ruben Gonzalez, Aaron Kaiser

SpeakerBio: Ruben Gonzalez, Neodyme

Crypto PhD, Security Researcher and Trainer at Neodyme

SpeakerBio: Aaron Kaiser

No BIO available

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

.EDU Community - Friday - 14:00-14:59 PDT

Title: Hacking Education - Teaching Offensive Cyber Science at the Collegiate Level

Tags: .EDU Community | Creator Talk/Panel

When: Friday, Aug 7, 14:00 - 14:59 PDT

Where: LVCCW Level 1 Hall 4 1418 (.EDU Community) - [Map](#)

Description:

SpeakerBio: Dave "Rebelcadet" Ortiz

David Ortiz is the Chief Technology Officer (CTO) at X8 LLC, where he leads the firm's engineering efforts to develop innovative technical, operational, and research solutions to meet complex customer requirements. With a diverse background in laser physics, information assurance, cyberspace operations, and organizational leadership, David is a seasoned professional dedicated to advancing cyber capabilities for both the U.S. Government and private industry customers.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Aerospace Village - Friday - 10:00-10:30 PDT

Title: Hacking Electronic Conspicuity Devices -or- Making Light Aircraft Fly Into Conflict

Tags: Aerospace Village | Creator Talk/Panel

When: Friday, Aug 7, 10:00 - 10:30 PDT

Where: LVCCW Level 1 Hall 3 1103 (Creator Stage 5) - [Map](#)

Description:

Commercial aircraft have Traffic Collision and Avoidance Systems, or TCAS, to ensure they don't fly in to each other, but these are very expensive systems. How do General Aviation aircraft find a way to avoid each other?

Enter 'Electronic Conspicuity' devices: small, light and cost effective sensors to detect other aircraft and alert GA pilots before they can be seen by the naked eye.

Unfortunately, in the rush to improve flight safety and situational awareness in GA, cyber security has taken something of a back seat. As a result, some of these EC devices have trivial and not-so-trivial security flaws. In some cases, it is possible to delete Traffic Advisories and/or give an incorrect Resolution Advisory, bringing planes in to conflict with each other, rather than ensuring they stay safely apart.

SpeakerBio: Ken Munroe

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Contests - Sunday - 10:00-11:59 PDT

Title: Hacking GRC Contest

Tags: Hacking GRC | Contest

When: Sunday, Aug 9, 10:00 - 11:59 PDT

Where: Online

Description:

Hacking CMMC is a hands-on cybersecurity competition designed to immerse participants in the practical aspects of the Cybersecurity Maturity Model Certification (CMMC). Through realistic, challenge-based scenarios, players explore common compliance gaps, security controls, and threats faced by defense contractors.

The CTF blends technical problem-solving with compliance-driven thinking, helping participants understand how security requirements translate into real-world incidents. It offers an engaging way to learn, test skills, and strengthen readiness for CMMC-aligned environments.

The CTF will be a Jeopardy-style CTF where every player will have a list of challenges in different categories. For every challenge solved, the player will get a certain number of points depending on the difficulty of the challenge.

Prerequisites

- Laptop with Internet Access

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Contests - Saturday - 10:00-17:59 PDT

Title: Hacking GRC Contest

Tags: Hacking GRC | Contest

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: Online

Description:

Hacking CMMC is a hands-on cybersecurity competition designed to immerse participants in the practical aspects of the Cybersecurity Maturity Model Certification (CMMC). Through realistic, challenge-based scenarios, players explore common compliance gaps, security controls, and threats faced by defense contractors.

The CTF blends technical problem-solving with compliance-driven thinking, helping participants understand how security requirements translate into real-world incidents. It offers an engaging way to learn, test skills, and strengthen readiness for CMMC-aligned environments.

The CTF will be a Jeopardy-style CTF where every player will have a list of challenges in different categories. For every challenge solved, the player will get a certain number of points depending on the difficulty of the challenge.

Prerequisites

- Laptop with Internet Access

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Contests - Friday - 10:00-17:59 PDT

Title: Hacking GRC Contest

Tags: Hacking GRC | Contest

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: Online

Description:

Hacking CMMC is a hands-on cybersecurity competition designed to immerse participants in the practical aspects of the Cybersecurity Maturity Model Certification (CMMC). Through realistic, challenge-based scenarios, players explore common compliance gaps, security controls, and threats faced by defense contractors.

The CTF blends technical problem-solving with compliance-driven thinking, helping participants understand how security requirements translate into real-world incidents. It offers an engaging way to learn, test skills, and strengthen readiness for CMMC-aligned environments.

The CTF will be a Jeopardy-style CTF where every player will have a list of challenges in different categories. For every challenge solved, the player will get a certain number of points depending on the difficulty of the challenge.

Prerequisites

- Laptop with Internet Access

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Hacking Hearts by Reverse Engineering Pacemaker Firmware

Tags: Biohacking Village | Creator Talk/Panel

When: Friday, Aug 7, 17:30 - 17:59 PDT

Where: LVCCW Level 1 Hall 3 1104 (Creator Stage 4) - [Map](#)

Description:

Gradually we are all becoming more and more dependent on connected technology. We will be able to live longer with an increased quality of life due to medical devices and sensors attached to, or integrated into our bodies. However, our dependence on technology grows faster than our ability to secure it, and a security failure of a medical device may cause patient harm and have fatal consequences.

This presentation dives into the security architecture of the Biotronik pacemaker ecosystem, covering the pacemaker, home monitoring units, and external programmer. Using a hybrid of black-box and white-box methodologies, we deconstruct the firmware and wireless communication protocols to identify vulnerabilities in a pacemaker that one of the presenters was depending on with their life for 11 years. We will discuss the challenges of extracting firmware from life-critical hardware and the implications of discovered bugs on patient safety. Attendees will leave with a better understanding of how to reverse engineer proprietary medical ecosystems and why securing the "Internet of Medical Things" is a race we cannot afford to lose.

Speakers: Marie Moe, Shayan Alinejad, Kristian Karlsen

SpeakerBio: Marie Moe

Dr. Marie Moe is a Principal Consultant at Mandiant (now part of Google Cloud), and has a PhD in information security. She is a part-time Associate Professor at NTNU. In this talk she will be joined by NTNU MSc students Shayan Alinejad and Kristian Karlsen.

SpeakerBio: Shayan Alinejad

No BIO available

SpeakerBio: Kristian Karlsen

No BIO available

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Bug Bounty Village - Friday - 16:00-16:59 PDT

Title: Hacking Human-in-the-Loop systems

Tags: Bug Bounty Village | Creator Talk/Panel

When: Friday, Aug 7, 16:00 - 16:59 PDT

Where: LVCCW Level 2 W206-207 (Bug Bounty Village) - [Map](#)

Description:

Customer support has always been a numbers game: high message volume, repetitive questions, and constant pressure to respond faster. Most organisations handle this through ticket portals, shared mailboxes or live chat tools. These systems were built around people reading messages and people taking action. That model is disappearing. To keep up with demand, support platforms now embed AI agents that read incoming messages, suggest replies, search internal knowledge pages and even interact with backend systems. They reset accounts, schedule refunds, modify settings and verify users before a human ever looks at the conversation. The human is still in the loop, but rarely in full control. Connecting a language model to business logic has a side effect. It turns text into a control layer. Messages no longer just inform a conversation; they influence actions. If an attacker can shape those messages, they can shape what the agent does. In security terms, that creates a new attack surface that did not exist when humans handled every request. This session examines how that surface is exploited in practice. The findings come from real vulnerability reports against production AI support systems that accept contact from the public. The attacks require no insider access. They target the assumptions that connect users, agents and operators, and they convert helpful automation into unintended system access. The examples that follow show how the trust built into these systems can be bent until it breaks.

SpeakerBio: Inti "securinti" De Ceukelaire, Founding Member, Intigriti

Intigriti is a Founding Member at Intigriti and their former Chief Hacker Officer. As a hacker, Inti has won multiple awards in live hacking competitions from Bugcrowd and HackerOne. Inti specialises in AI-hacking techniques, logic flaws and support systems, and is most known for the "Ticket Trick" methodology that has earned a spot in Portswigger Top Web Hacking Techniques.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Bug Bounty Village - Friday - 10:30-11:30 PDT

Title: Hacking IDE Extensions - VSCode Workshop

Tags: Bug Bounty Village | Creator Workshop

When: Friday, Aug 7, 10:30 - 11:30 PDT

Where: LVCCW Level 2 W206-207 (Bug Bounty Village) - [Map](#)

Description:

IDE extensions are a lucrative slice of the modern bug bounty scope. They run with privileged capabilities, parse arbitrary workspace files, and increasingly ship LLM backed agentic features that execute commands, edit files, and follow instructions found in the project under review. AI assistants have become an exploit chain accelerator: agents touch every stage from file ingestion to primitive acquisition to escalation, often with minimal sandboxing. This workshop turns those ideas into hands on practice. Attendees install "Nopilot", a deliberately vulnerable mock AI assistant VS Code extension, learn how to debug it, review code for bugs, and chain primitives from "user opened a folder" to code execution that requires no further interaction and bypasses workspace trust entirely. Built around a generalized IDE exploitation killchain and drawn from a multi-six-figure IDE bug bounty practice. Bring a laptop and curiosity. Read the full description here:

<https://gist.github.com/nickcopi/daf5b24b262c802830ab6c1ef9d5d49d>

SpeakerBio: Nick "7urb01" Copi

Nick Copi is a full-time bug bounty hunter targeting web applications, cloud infrastructure, desktop apps, and pretty much anything with an attack surface. His background spans application security engineering, full-stack development, and a long track record of local CTF competition wins. He has presented several technical talks at security conferences and regularly publishes and reviews security research. He really likes JavaScript. Maybe too much. Maybe someone should check on him.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Hacking iOS Apps in a Structured Way

Tags: Mobile Hacking Community | Creator Event/Activity

When: Saturday, Aug 8, 13:15 - 14:45 PDT

Where: LVCCW Level 1 Hall 4 1422 (Mobile Hacking Community) - [Map](#)

Description:

Mobile app testing has many pitfalls and a structured approach is needed to get a holistic picture of the attack surface. The OWASP Mobile Application Security (MAS) project is able to support you with that. In this workshop, you'll get a practical introduction to the MAS ecosystem which consists of the standard, mobile weaknesses and how to test them. You will experience test cases and demos for iOS in action for static and dynamic analysis, and learn how to perform a mobile penetration test on a non-jailbroken iOS device.

By the end of the workshop, attendees will be able to: - Navigate the OWASP Mobile Application Security (MAS) project (MASVS, MASWE, MASTG) and locate relevant test cases for their own engagements. - Apply a mix of static and dynamic analysis techniques against real iOS apps. - Use the right tooling (e.g. frida, radare2, AI-assisted reverse engineering) in their pentest workflow.

Instructions: <https://github.com/sushi2k/defcon34-ios-workshop>

Prerequisites: a laptop with 10 GB free disk space; GitHub account and git installed.

SpeakerBio: Sven Schleier, Co-Founder at Bai7 GmbH

Sven has been involved with the Open Worldwide Application Security Project (OWASP) since 2016. As a co-project lead and author, he has made significant contributions to the OWASP MAS (Mobile Application Security) project, which is considered the industry standard for mobile application security, see <https://mas.owasp.org>.

Sven is a frequent speaker and trainer around the world. His audiences range from software developers to students and penetration testers. His engagements often take him to conferences, forums and educational institutions, where he shares his extensive knowledge and insights on mobile and application security.

--

Sven is a co-founder of Bai7 GmbH in Austria, which is specialized in trainings and advisory. He has expertise in cloud security, offensive security engagements (Penetration Testing) and Application Security, notably in guiding software development teams across Mobile and Web Applications throughout the Software Development Life Cycle (SDLC) to integrate robust security measures in from the start.

Besides his day job, Sven is involved with the Open Worldwide Application Security Project (OWASP) since 2016. As a co-project leader and author, he has significantly contributed to the OWASP Mobile Application Security Testing Guide (MASTG) and the OWASP Mobile Application Security Verification Standard (MASVS).

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Hacking Jetskis - from Sea-Don't to Sea-Doo

Tags: DEF CON Official Talk | Demo | Tool

When: Sunday, Aug 9, 14:00 - 14:30 PDT

Where: LVCCW Level 1 Hall 3 903 (Main Track 5) - [Map](#)

Description:

One day, I woke up to a simple message from a friend: "What do you know about CAN bus?" Expecting him to have car trouble, I called him and asked, "What do you need?"

Turns out the car trouble was actually jetski trouble: he bought a Sea-Doo jetski for very cheap - but it came without a key. A quick research on his side showed that the jetski does not (like others from the time) use a simple magnet key: No, the jetski has a full, digital immobilizer system, and just the tools to diagnose and program in a new key cost more than the jetski. And zero public information is available on how this all works.

And so we dove in: from reverse-engineering the CAN bus diagnostics protocol and the electronic key protocol to designing our own freely programmable key and a Flipper Zero jetski diagnostic app, this talk goes into the weeds of hacking something that I didn't even know needed to be hacked: Jetskis!

SpeakerBio: stacksmashing, hextree.io

Thomas Roth aka stacksmashing is a security researcher mostly focused on hardware and firmware. His work includes hardware attacks on processors & microcontrollers, building cheap JTAG tooling for the iPhone, and attacking a wide variety of embedded devices. He also runs a YouTube channel called stacksmashing about security, reverse engineering and hardware hacking.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Hacking the EOD Bot: How I Learned to Stop Worrying and Love the Boomba

Tags: DEF CON Official Talk | Demo | Exploit

When: Friday, Aug 7, 16:00 - 16:59 PDT

Where: LVCCW Level 1 Hall 3 903 (Main Track 5) - [Map](#)

Description:

What happens when you wander into a surplus store and walk out with a bomb disposal robot? You name him “Boomba” and tear him apart. Built by Roomba creator iRobot, the PackBot is often used by agencies who need to deploy a small, ruggedized robot in potentially dangerous locations. But beneath its rugged shell lies a fascinating time capsule of early 2000s engineering. As the platform's physical capabilities evolved to meet extreme operational demands, its core software trailed behind, relying on legacy hardware and an architecture built before modern security controls. This talk is a full-stack teardown of a six-figure tactical asset. We'll explore its 25-year evolution: mapping undocumented interfaces, fabricating custom cables, and replacing legacy 4.9 GHz restricted-band radios with custom hardware. We will dive into the software to expose unencrypted VPN connections and entirely plaintext Python 2.5 control protocols. We will also demonstrate vulnerabilities that grant full root access. Finally, we'll decompile its modern tablet control app, breaking down the JAUS protocol to reveal a critical command injection vulnerability. With a live PackBot on stage, we'll intercept telemetry, pop the LFI, and eavesdrop on network traffic. Watch Boomba get turned back into a vacuum, and catch him later at the Car Hacking

Speakers: Patrick "gigstorm" Kiley, Emily "@astradotpng" Astranova

SpeakerBio: Patrick "gigstorm" Kiley, Google

Patrick Kiley is a Security Consultant doing embedded security testing and has over 20 years of information security experience. Patrick has performed research in avionics security, vehicles, and even managed to brick his Tesla making it go faster. Patrick has a patent pending on an embedded security access tool and loves tearing things apart while figuring out how they work.

SpeakerBio: Emily "@astradotpng" Astranova, Google

Emily is a security consultant doing physical security testing, covert entry and penetration testing of all the things. Emily has intentionally compromised US power grid systems, unintentionally compromised data centers and has somehow managed to keep her record to only one run-in with the FBI. In her spare time, Emily volunteers as a software and cybersecurity mentor for high school students as a part of FIRST Robotics.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Hacking the Government: How Two Researchers Turned Late-Night Boredom Into a National Audit

Tags: DEF CON Official Talk

When: Friday, Aug 7, 12:30 - 12:59 PDT

Where: LVCCW Level 1 Hall 3 903 (Main Track 5) - [Map](#)

Description:

What happens when two researchers spend several days scrutinizing the Polish web? We didn't just find anomalies—we took action. Join us as we reveal the results of our intensive research, which led to multiple official reports to CSIRT GOV, NASK, and MON. We will walk you through our findings, the scale of the threats discovered, and provide essential recommendations for a more secure digital future.

Speakers: Robert "ProXy" Kruczek, Kamil Szczurowski

SpeakerBio: Robert "ProXy" Kruczek, Securitum

I am a Cybersecurity Consultant, Mentor, and Ethical Hacker (known in the infosec community as ProXy) at Securitum - Poland's leading cybersecurity firm - and a contributor to [sekurak.pl](#), the country's largest infosec portal. With over 10 years of experience in vulnerability research and penetration testing.

Operating under the ProXy alias, I discovered and reported 43 CVEs and I am an active Bug Bounty hunter (Hall of Fame at OLX, reports for BlaBlaCar, OVH, and ERCOM).

SpeakerBio: Kamil Szczurowski, Securitum

On a daily basis, Kamil Szczurowski specializes in web application security testing and social engineering assessments. In his free time, he analyzes malware, APT campaigns, open-source software, and software used by government institutions, which has resulted in multiple CVE entries and publications. He is also an author of articles published on [sekurak.pl](#).

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Hacking the Hackers who Hack Hackers: Supply-Chain Backdoors in Underground VPN Infrastructure

Tags: DEF CON Official Talk

When: Friday, Aug 7, 15:00 - 15:59 PDT

Where: LVCCW Level 1 Hall 3 903 (Main Track 5) - [Map](#)

Description:

Underground VPN and tunneling ecosystems are widely used to monetize compromised servers and sell “free internet” access through SSH, SOCKS, and multi-protocol tunnels. These operations rely heavily on open-source infrastructure management tools deployed on rented or hacked Linux servers. But what happens when the tools themselves are weaponized?

In this talk we dissect FirewallFalcon Manager, a VPN/SSH server management toolkit widely promoted in Telegram communities. While it presents itself as a legitimate open-source platform, our analysis reveals a multi-layered supply-chain attack targeting the very operators who deploy it.

FirewallFalcon silently installs backdoors, injects a rogue TLS root certificate, hijacks DNS resolution, and redirects proxy traffic through attacker-controlled infrastructure to enable large-scale Man-in-the-Middle interception. Earlier versions also deployed a Telegram reconnaissance bot and a universal SSH backdoor granting root access to infected servers.

Using reverse engineering, GitHub history analysis, DNS infrastructure mapping, and large-scale internet scanning, we uncovered hundreds of active servers inside this compromised ecosystem. This talk exposes a new class of supply-chain attacks: hackers hacking the infrastructure used by other hackers.

SpeakerBio: Assaf Morag, Flare

Assaf Morag is a Cybersecurity Researcher and Threat Intelligence Consultant, working with various companies on research focused on underground ecosystems, attacker infrastructure, and the evolving cyberthreat landscape. His work translates adversary activity from open, deep, and dark-web sources into actionable intelligence for security teams and the software development life cycle. Previously, Assaf served as Director of Threat Intelligence at Aqua Security and held senior intelligence roles at BlueVoyant and IBM Security. His research has been featured in leading cybersecurity publications and presented at major industry conferences. He contributed to the MITRE ATT&CK® Container Framework and authored an O'Reilly course on cloud-native cyber threat intelligence.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Red Team Village - Sunday - 13:00-13:59 PDT

Title: Hacking the Human-in-the-Loop

Tags: Red Team Village | Misc

When: Sunday, Aug 9, 13:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 1 309 (Red Team Village) Workshop Stage 2 - [Map](#)

Description:

AI defenses are only as good as the analysts training them. This session exposes how attackers manipulate SOC analyst behavior to silently degrade AI baselines over time, no exploit required. We cover the mechanics of false positive injection, alert fatigue as a weapon, and misdirection. Then attendees step into the analyst's seat in a live browser-based simulation and experience how their own decisions poison the model.

Speakers: Alexander "Zombie", Lee McWhorter

SpeakerBio: Alexander "Zombie"

4.5 years in the SOC. Junior Analyst to Team Lead. CPTS, CRT0, CRTE, OSCP and enough certs to wallpaper a small room with some left over. Zombie has spent the better part of half a decade watching how defenders think, how they triage, how they get tired, and how attackers can weaponize all three. By day he leads a SOC team. By night he's learning everything he can about breaking the things he built. Still technically blue team. Emphasis on technically.

SpeakerBio: Lee McWhorter

Lee McWhorter, Owner & Chief Geek at McWhorter Technologies, has been involved in IT since his early days and has over 30 years of experience. He is a highly sought after professional who first learned about identifying weaknesses in computer networks, systems, and software when Internet access was achieved using a modem. Lee holds an MBA and more than 20 industry certifications in such areas as System Admin, Networking, Programming, Linux, IoT, and Cybersecurity. His roles have ranged from the server room to the board room, and he has taught for numerous universities, commercial trainers, and nonprofits. Lee is the SWAG Master and a Core Staff member for the Red Team Village at DEFCON; and works closely with the Pacific Hackers Association, Dark Arts Village at RSAC, Texas Cyber Summit, CompTIA, and the CompTIA Instructor Network as a Speaker, SME, and Instructor.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Hacking Your Life with AI Can Get You Hacked: How AI Orchestration Platforms Ship RCE by Design

Tags: DEF CON Official Talk | Demo | Exploit

When: Saturday, Aug 8, 16:00 - 16:59 PDT

Where: LVCCW Level 1 Hall 3 1006 (Main Track 1) - [Map](#)

Description:

AI orchestration platforms promise to automate your life. They deliver, just not always for you. Kestra, Langflow, Nocobase, Flowise, Activepieces, Dify, and Apache Airflow have quietly become critical infrastructure, and they all share the same dangerous assumption: anyone who can touch a workflow is trusted to run code on the host. I went hunting across seven major platforms and walked out with multiple CVEs and critical-severity findings. I'll share an arsenal of RCE primitives: shell injection through template rendering, `exec()` on user-supplied "validation" code, `eval()` on raw LLM output, and unauthenticated API endpoints that hand you a shell. Then I'll demonstrate the kill shot: an unauthenticated attacker achieving full RCE through a single prompt injection into an LLM module. When I reported these, some vendors told me code execution is intended behavior and security is the deployer's problem. I'll show you why that argument falls apart in real deployments, and walk through the trust boundary failures that keep producing the same bugs across the ecosystem. You'll leave with a methodology for tearing these platforms apart, a catalog of recurring vulnerability patterns, and a framework for evaluating whether a platform's threat model survives contact with reality.

SpeakerBio: Peyton "p80n-sec" Kennedy, Endor Labs

Peyton 'p80n-sec' Kennedy is a Senior Security Researcher at Endor Labs, where he focuses on offensive security research, vulnerability discovery, and exploit development against the open source projects shaping modern software. His research has produced CVE disclosures across widely deployed frameworks and platforms, including koa.js and openclaw, with a consistent focus on the gap between what platforms claim about their threat models and what they actually enforce.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Haetae: An Agent to Takedown North Korean C2 Servers

Tags: Adversary Village | Creator Talk/Panel

When: Friday, Aug 7, 11:30 - 11:59 PDT

Where: LVCCW Level 1 Hall 3 1105 (Creator Stage 3) - [Map](#)

Description:

In this talk, we introduce Haetae, an agent designed to profile, identify, and exploit C2 frameworks used by North Korean malware.

Haetae supports both automated and interactive modes, allowing analysts to map and understand adversary infrastructure with different levels of control. It is built around a flexible rule-based system, enabling users to extend and refine detections as new patterns and frameworks emerge.

In this first release, we will walk through real-world cases where Haetae was used to identify and take down infrastructure associated with Mach-O Man and POWERful Armadillo.

We will also release a safe emulator of both malware C2 servers, allowing researchers and newcomers to experiment with Haetae in realistic, controlled environments without risk.

This is a highly technical talk but can be enjoyed by both beginners and seasoned threat hunters.

Speakers: Mauro Eldritch, Nelson Rafael Colón Merán

SpeakerBio: Mauro Eldritch, Leader at Bitso Quetzal Team

Hacker and Speaker.

Founder of BCA LTD and DC5411.

I wrote a book interviewing Threat Actors.

I like Threat Intelligence and Golden Retrievers.

SpeakerBio: Nelson Rafael Colón Merán, Security Engineer at Bitso

Security Engineer at Bitso, Latin America's leading crypto-first financial platform. I've specialized in red team operations, penetration testing, and malware development.

Recognized speaker in the Dominican Republic's RedTeamRD cybersecurity community, where I've given a couple talks and previously assisted DEFCON as a speaker.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Red Team Village - Friday - 16:00-17:59 PDT

Title: Haetae: An Agent to Takedown North Korean C2 Servers

Tags: Red Team Village | Misc

When: Friday, Aug 7, 16:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 309 (Red Team Village) Tactic Table 3 - [Map](#)

Description:

In this talk, we introduce Haetae, an agent designed to profile, identify, and exploit C2 frameworks used by North Korean malware.

Haetae supports both automated and interactive modes, allowing analysts to map and understand adversary infrastructure with different levels of control. It is built around a flexible rule-based system, enabling users to extend and refine detections as new patterns and frameworks emerge.

In this first release, we will walk through real-world cases where Haetae was used to identify and take down infrastructure associated with Mach-O Man and POWERful Armadillo.

We will also release a safe emulator of both malware C2 servers, allowing researchers and newcomers to experiment with Haetae in realistic, controlled environments without risk.

This is a highly technical talk but can be enjoyed by both beginners and seasoned threat hunters.

Speakers: Mauro Eldritch, Nelson Rafael Colón Merán

SpeakerBio: Mauro Eldritch, Leader at Bitso Quetzal Team

Hacker and Speaker.

Founder of BCA LTD and DC5411.

I wrote a book interviewing Threat Actors.

I like Threat Intelligence and Golden Retrievers.

SpeakerBio: Nelson Rafael Colón Merán, Security Engineer at Bitso

Security Engineer at Bitso, Latin America's leading crypto-first financial platform. I've specialized in red team operations, penetration testing, and malware development.

Recognized speaker in the Dominican Republic's RedTeamRD cybersecurity community, where I've given a couple talks and previously assisted DEFCON as a speaker.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Malware Village - Saturday - 11:35-12:15 PDT

Title: Haetae: An Agent to Takedown North Korean C2 Servers

Tags: Malware Village | Creator Talk/Panel

When: Saturday, Aug 8, 11:35 - 12:15 PDT

Where: LVCCW Level 1 Hall 2 600 (Malware Village) Talks - [Map](#)

Description:

In this talk, we introduce Haetae, an agent designed to profile, identify, and exploit C2 frameworks used by North Korean malware.

Haetae supports both automated and interactive modes, allowing analysts to map and understand adversary infrastructure with different levels of control. It is built around a flexible rule-based system, enabling users to extend and refine detections as new patterns and frameworks emerge.

In this first release, we will walk through real-world cases where Haetae was used to identify and take down infrastructure associated with Mach-O Man and POWERful Armadillo.

We will also release a safe emulator of both malware C2 servers, allowing researchers and newcomers to experiment with Haetae in realistic, controlled environments without risk.

This is a highly technical talk but can be enjoyed by both beginners and seasoned threat hunters.

SpeakerBio: Nelson Colon, Offensive Security Specialist at Bitso Quetzal Team

Dominican Offensive Security Specialist. I spoke at DEF CON Data Duplication Village about creating immortal C2 servers using modern data duplication platforms.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Social Gatherings/Events - Thursday - 10:00-16:59 PDT

Title: Ham In A Day Class

Tags: Event | Ham Radio Village

When: Thursday, Aug 6, 10:00 - 16:59 PDT

Where: LVCCW Level 3 W314 (Ham Radio Meeting) - [Map](#)

Description:

The HRV Ham In A Day class returns again for its fourth year, taught again by Dan Romencheck, KB6NU, author of the No-Nonsense Study Guides for the amateur radio license exams.

Always been interested in getting your ham license but never had the time to study? Now's your chance! The Ham Radio Village is offering a one-day class where you can learn all the required knowledge to pass the exam.

Topics include: - Electrical Principles - Electronic principles and components - Radio and electromagnetic wave properties - Antennas and Feedlines - Amateur Radio Signals - Safety - Station Setup and Operation -Operating Procedures - Rules and Regulations

The class will run from 10 A.M. to 5 P.M. A lunch break will be provided.

Best of all, this class is completely free, thanks to a grant from the Amateur Radio Digital Communications.

Last year, we sold out of capacity and had to turn folks away. We highly recommend placing a deposit to reserve your seat. The deposit will be refunded upon attendance of the class. Register by following the attached link.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Ham Radio Village - Saturday - 14:30-14:59 PDT

Title: Ham Radio - Licensed to Experiment

Tags: Ham Radio Village | Creator Talk/Panel

When: Saturday, Aug 8, 14:30 - 14:59 PDT

Where: LVCCW Level 3 W315 (Ham Radio Village) - [Map](#)

Description:

The most common question we hear in the village is, "What can I do now that I'm licensed?" N0OPS and W0BDP attempt the guide new hams into incorporating ham radio into their current hobbies or pursuing new interests.

N0OPS and W0BDP will walk the audience through the diversity of ham radio operations such as portable activations such as POTA/SOTA, satellite contacts, digital weak-signal modes, direction-finding competitions, emergency communications, and drone telemetry.

The takeaway: no matter how long you've held a call sign whether it's 5-minutes or 5 years, there's almost certainly a corner of this hobby you haven't touched yet. This speech is an invitation to go find it.

SpeakerBio: Dan W0BDP Norte

Dan "darkestofdans" Norte (W0BDP) is a penetration tester, currently with NetSPI. Dan has been a ham radio operator for 9 years, currently Amateur Extra class. Dan enjoys popping shells and chasing DX.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Ham Radio Isn't Magic: Preppers, Sad Hams, and Practical Off-Grid Communications

Tags: Ham Radio Village | Creator Talk/Panel

When: Friday, Aug 7, 13:00 - 13:59 PDT

Where: LVCCW Level 3 W315 (Ham Radio Village) - [Map](#)

Description:

This talk approaches off-grid communications as a practical systems problem, informed by the author's real-world operation of portable and off-grid radio systems rather than theory or gear marketing. Rather than teaching amateur radio as a hobby, it reframes off-grid communications using failure-mode analysis and systems design principles familiar to the security and hacking community. While the question "How do I talk 500 miles when the grid is down?" is a common starting point, the deeper issue is how communication systems behave when infrastructure is absent, degraded, or intentionally avoided — and why many well-intentioned plans fail in practice.

The presentation is structured as a 101-level introduction for a technically curious audience. It assumes no prior amateur radio experience, but it does assume interest in understanding constraints, tradeoffs, and failure modes the same way hackers evaluate any other system operating outside ideal conditions.

The talk opens by examining real examples from off-grid and preparedness communities, including common questions and the unhelpful responses they often attract. This framing establishes the core thesis: both "prepper fantasy" and "sad ham" gatekeeping optimize for the wrong constraints and lead to brittle designs that fail when conditions are imperfect.

From there, the talk builds a mental model of off-grid radio communications grounded in physics and operational reality. Attendees are introduced to why radio performance is probabilistic rather than guaranteed, why a fixed distance like "500 miles" is a misleading requirement, and how factors such as propagation, noise floor, antenna efficiency, duty cycle, and coordination dominate outcomes more than transmitter power or radio model. Real failure modes are discussed, including HF voice links failing when expected to work, digital modes succeeding where voice does not, antenna quality overwhelming other variables, high-noise environments negating otherwise capable setups, and situations where increasing power does not meaningfully improve reliability.

The scope then expands beyond emergencies to everyday off-grid use cases hackers actually encounter: group communications while hiking or camping without cell coverage, portable and battery-powered operation, short-range mesh and store-and-forward systems such as Meshtastic, and longer-range low-bandwidth HF messaging. Activities like Parks on the Air, Summits on the Air, and Field Day are presented not as hobbies, but as structured opportunities for exploration and experimentation — real-world environments for testing antennas, power systems, logistics, and coordination under off-grid constraints.

Rather than focusing on specific products or modes, the talk emphasizes design principles that consistently work: simple plans over clever ones, redundancy across bands and modes, asynchronous messaging over real-time voice, and communication plans that account for human behavior as a primary constraint. Regulatory considerations are covered at a practical level to help attendees understand what is possible and appropriate without turning the talk into a licensing lecture.

If appropriate for the venue, the talk may include a short demonstration or case study illustrating propagation variability or the effectiveness of low-bandwidth digital techniques compared to voice. Any demonstration will be designed with realistic fallback options and framed as illustrative rather than guaranteed.

The goal of this talk is not to turn attendees into radio experts, but to give them a reusable framework for thinking about off-grid communications the way hackers think about resilient systems: define the actual problem, understand how and why things fail, and design solutions that work in imperfect, real-world environments.

Every hacker has seen the post: someone asks what radio will let them “reliably talk 500 miles to family when the cell network goes down.” The replies quickly devolve into bad advice, magical thinking, and dismissive gatekeeping. The result is confusion, wasted money, and false confidence about off-grid communications.

This talk is the antidote.

We’ll cut through the mythology and explain what amateur radio can actually do for personal and family communication during major disruptions — and what it cannot. Starting at a 101 level, we’ll cover realistic ranges, basic propagation, equipment tradeoffs, digital modes, licensing myths, and why distance is usually the wrong requirement.

Rather than dunking on preppers or policing fun like a sad ham, this talk reframes the problem the way hackers do: understanding constraints, failure modes, and human factors.

We’ll focus on practical off-grid communication strategies that work in the real world — coordination, redundancy, and low-bandwidth messaging — not fantasy continent-spanning voice links.

SpeakerBio: Andrew Ohnstad - N3OCQ

Andrew has spent 25 years designing large-scale IT systems. He grew up alongside the birth of the internet, building his own computers, running a BBS, and taking electronics apart to understand how they worked. His interests remain firmly hands-on, focused on hardware tinkering and RF. He’s been a licensed amateur radio operator since 1993, holds an Amateur Extra license, and is active from VHF/UHF through 160 meters.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

The Diana Initiative - Friday - 11:00-11:10 PDT

Title: Ham Radio Village Tour

Tags: The Diana Initiative | Creator Tour

When: Friday, Aug 7, 11:00 - 11:10 PDT

Where: LVCCW Level 1 South Lobby / Atrium - [Map](#)

Description:

Interested in visiting Ham Radio Village but afraid to go by yourself? The Diana Initiative is hosting tours! Follow a volunteer to Ham Radio Village and be introduced to the community and activities inside!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Hands-On Autonomous Pentesting with Pentest Copilot

Tags: Red Team Village | Misc

When: Saturday, Aug 8, 10:00 - 11:59 PDT

Where: LVCCW Level 1 Hall 1 309 (Red Team Village) Tactic Table 4 - [Map](#)

Description:

Pentest Copilot is an MIT licensed open-source agentic penetration testing workspace designed to assist security professionals with web/network application assessments.

This hands-on tactic introduces participants to operating autonomous web pentesting workflows against intentionally vulnerable applications. Attendees will deploy Pentest Copilot, configure the environment, and use it to perform attack-surface discovery, authenticated testing, vulnerability investigation, and workflow-driven analysis.

Rather than focusing on theory, the session is designed around practical offensive workflows. Participants will observe how autonomous agents navigate modern web applications, identify interesting attack paths, investigate findings, and assist with security testing tasks that traditionally require significant manual effort.

The goal is to provide attendees with a realistic understanding of how autonomous systems can augment offensive security work today, where they are effective, and where human operators remain essential.

Pentest Copilot is fully open source and available at: <https://github.com/bugbasesecurity/pentest-copilot>, Wiki is at: <https://github.com/bugbasesecurity/pentest-copilot/wiki> over 800+ stars.

Speakers: Dhruva Goyal, Sitaraman Subramanian

SpeakerBio: Dhruva Goyal

Dhruva has been hacking since middle school and enjoys offensive security research and red teaming. Dhruva is certified with OSCE3 (ie. OSWE, OSEP & OSED) and OSCP. He leads the cybersecurity engagements and triage team at BugBase. He also loves playing AOE4 and working out.

SpeakerBio: Sitaraman Subramanian

Sitaraman Subramanian is the CTO at BugBase. He has spent over five years working in offensive security and over a decade building products. His work spans full stack development, DevSecOps, cloud security, and offensive security. He built BugBase from the ground up, and now leads engineering on Pentest Copilot, an autonomous AI driven pentesting platform. He presented at Black Hat USA Arsenal in 2025 and Microsoft BlueHat in 2024. He is an active open source contributor. Pentest Copilot is open sourced at <https://github.com/bugbasesecurity/pentest-copilot>, with 850+ stars and growing. He writes about hacking and AI evals at <https://blog.ssitaraman.com>.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

IoT Village - Saturday - 10:00-17:59 PDT

Title: Hands-On Hardware Hacking – From JTAG to Root, Memory Patching Boot Process for Root Access

Tags: IoT Village | Creator Workshop

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 215 (IoT Village) - [Map](#)

Description:

Using tools like OpenOCD and Segger J-Link Mini, we'll guide you through modifying the boot 'init=' process in memory via JTAG, forcing the device into a single user mode shell via UART.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

IoT Village - Friday - 10:00-17:59 PDT

Title: Hands-On Hardware Hacking – From JTAG to Root, Memory Patching Boot Process for Root Access

Tags: IoT Village | Creator Workshop

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 215 (IoT Village) - [Map](#)

Description:

Using tools like OpenOCD and Segger J-Link Mini, we'll guide you through modifying the boot 'init=' process in memory via JTAG, forcing the device into a single user mode shell via UART.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

IoT Village - Sunday - 10:00-13:59 PDT

Title: Hands-On Hardware Hacking – From JTAG to Root, Memory Patching Boot Process for Root Access

Tags: IoT Village | Creator Workshop

When: Sunday, Aug 9, 10:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 1 215 (IoT Village) - [Map](#)

Description:

Using tools like OpenOCD and Segger J-Link Mini, we'll guide you through modifying the boot 'init=' process in memory via JTAG, forcing the device into a single user mode shell via UART.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Recon Village - Friday - 10:00-12:30 PDT

Title: Hands-On Supply Chain Recon & Vendor Risk Mapping

Tags: Recon Village | Creator Workshop

When: Friday, Aug 7, 10:00 - 12:30 PDT

Where: LVCCW Level 1 Hall 2 501 (Recon Village) - [Map](#)

Description:

Every organization relies on third-party vendors, open-source packages, and CI/CD tools to build and deliver software. In this session, we'll learn how to identify and map these external dependencies, understand the trust relationships between them, and discover potential security risks. Through practical demonstrations, attendees will see how issues such as dependency confusion, insecure GitHub Actions workflows, and vendor-related weaknesses can become entry points for supply chain attacks. The goal is to help security teams find and fix these risks before attackers do.

Speakers:Dhiyaneshwaran Balasubramaniam,Aman Rawat

SpeakerBio: Dhiyaneshwaran Balasubramaniam

No BIO available

SpeakerBio: Aman Rawat

No BIO available

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Maker's Village - Friday - 12:00-12:59 PDT

Title: Hardhat How-to

Tags: Maker's Village | Hard Hat Brigade | Creator Event/Activity

When: Friday, Aug 7, 12:00 - 12:59 PDT

Where: LVCCW Level 1 Hall 1 301 (Makers' Village) - [Map](#)

Description:

Do you like hats? Hard Hat Brigade likes hats! Come hang with MrBill and m0nkeydrag0n as we work on building a hard hat and problem solve the build together. See you soon!

Speakers:m0nkeydrag0n,MrBill

SpeakerBio: m0nkeydrag0n

No BIO available

SpeakerBio: MrBill

No BIO available

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Harvest Now, Decrypt Later: Practical Attacks on Post-Quantum Cryptography Implementations

Tags: DEF CON Official Talk | Demo | Tool

When: Saturday, Aug 8, 10:30 - 11:30 PDT

Where: LVCCW Level 1 Hall 3 1007 (Main Track 2) - [Map](#)

Description:

Post-quantum cryptography is being deployed to defeat a computer that doesn't exist yet - and the rush is opening a wide, purely classical attack surface today. This talk walks three implementation attack vectors against NIST's lattice standards (ML-KEM / FIPS 203, ML-DSA / FIPS 204): (1) memory corruption at the deserialization boundary, culminating in remote code execution through a hybrid TLS 1.3 key exchange; (2) compiler-induced timing side channels, where "constant-time" source becomes variable-time binary and yields a chosen-ciphertext key-recovery oracle; and (3) fault injection against ML-DSA's signing state machine on a low-cost ChipWhisperer. No quantum computer is required for any of them. The talk closes with the limits of hybrid cryptography as a defense and the live release of LatticeScope, an open-source timing-leak detector and lattice-aware fuzzer for auditing compiled PQC binaries.

SpeakerBio: Aleksandr Krasnov

Aleksandr has been an industry expert in DevSecOps, has worked in companies like Dropbox, Palo Alto Networks, and Meta/Facebook. He has spent his time doing security research and holds several patents in the area of application security. In the free time, Aleksandr spends time exploring the great outdoors in British Columbia, climbing new boulders, or free diving in the ocean.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Bug Bounty Village - Sunday - 11:30-11:59 PDT

Title: Heavy Metal and Hidden Secrets: A Five-Year Retrospective on DEF CON Challenge Coins

Tags: Bug Bounty Village | Creator Talk/Panel

When: Sunday, Aug 9, 11:30 - 11:59 PDT

Where: LVCCW Level 2 W206-207 (Bug Bounty Village) - [Map](#)

Description:

Take a look behind the scenes at five years of custom DEF CON challenge coins from DEF CON 30 through DEF CON 34. This session walks through the entire lifecycle of these unique hardware puzzles, exploring the inspiration behind their designs, step-by-step solutions, and how the rise of AI is shifting the future of cryptographic challenges.

SpeakerBio: Ariel "arl_rose" Garcia

Ariel Garcia (arl_rose) is a security researcher with over a decade of experience in pentesting, bug bounty, and cybersecurity community building. Blending hands-on offensive security with deep community ties, his work is a driving force within the hacker ecosystem. He has organized multiple Live Hacking Events, co-founded the global Ambassador World Cup, and led community initiatives spanning content creation, Discord management, and security instruction. A DEF CON attendee since 2014, Ariel is the co-founder of the Bug Bounty Village, providing a dedicated space to support the researchers and organizations shaping the field.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Hey Adversary, I've Got a Human EDR Bypass for You...

Tags: Adversary Village | Creator Talk/Panel

When: Friday, Aug 7, 15:15 - 15:45 PDT

Where: LVCCW Level 1 Hall 3 1105 (Creator Stage 3) - [Map](#)

Description:

Subtitle: The Scout's Field Guide to human risk telemetry: Weaponizing complacent corporate conditioning, tracking the legacy Human EDR, and surviving the wilderness.

Enterprise security leadership is currently suffering from a dangerous cognitive bias: confusing compliance with operational resilience. When an organization achieves a "1.5% phishing click-rate," the board celebrates under the illusion that their perimeter is secure. But to an advanced adversary, that dashboard isn't a shield it's a deterministic roadmap of the target's behavioral heuristics.

Framed as a retro-futuristic, illustrated Scout's Field Guide, this talk exposes how advanced Red Teams and APT actors reverse-engineer corporate human risk telemetry to achieve rapid initial access without advanced code. We will dissect how standardized training inadvertently programs a rigid "Human EDR" based on static signatures, and how operators can fly beneath the radar by simply omitting what the user has been conditioned to look for.

Furthermore, we will unlock a highly unique, unexplored exploitation vector: Behavioral Inheritance (The Legacy Human EDR). Attendees will learn how to conduct passive OSINT on a high-value target's professional history to predict their automated reactions, weaponizing the cognitive conditioning they inherited from their previous employers to bypass structural controls during their onboarding window.

Instead of chasing compliance or deploying new tools, this presentation concludes by turning offensive telemetry into zero-cost tactical defense. We will demonstrate how to evolve from static detection to pure behavioral resilience by implementing "Interrupt Protocols" to break an attacker's live performance, and adopting a "No-Fault Reporting" culture to drastically reduce adversary dwell time. We are unifying Red Team tradecraft with existing human telemetry to survive the corporate wilderness using the adversary's own playbook against them.

SpeakerBio: Daniel Isler, Awareness & Social Engineering Consultant - Team Leader - SEK

Daniel Isler, holds a Bachelor's degree in Performing Arts, weaponizing his background in theatrical representation, pretexting, and human behavior to reverse-engineer corporate conditioning. Active in the offensive security field since 2015, he serves as the Team Leader of Friendly RATs, the specialized social engineering and initial access for Red Team unit at SEK. Certified in OSINT, Red Team, and Social Engineering, he has spent nearly a decade architecting both high-fidelity tactical intrusions and enterprise Awareness service lines. His unique approach relies on a multidisciplinary, highly creative team of elite operators who strictly design and deliver educational content based on the advanced threat techniques they actively execute in the field.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

The Diana Initiative - Friday - 11:40-11:50 PDT

Title: HHV/SSV Tour

Tags: The Diana Initiative | Creator Tour

When: Friday, Aug 7, 11:40 - 11:50 PDT

Where: LVCCW Level 1 South Lobby / Atrium - [Map](#)

Description:

Interested in visiting HHV/SSV but afraid to go by yourself? The Diana Initiative is hosting tours! Follow a volunteer to HHV/SSV and be introduced to the community and activities inside!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: High Voltage Heist: Turning Your EV into my Power Bank

Tags: DEF CON Official Talk | Demo | Tool

When: Saturday, Aug 8, 17:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 3 1006 (Main Track 1) - [Map](#)

Description:

Ever found yourself with a dead phone battery in a Walmart parking lot? What if we told you that you could walk up to a parked EV and charge your phone directly from its traction battery - no authorization, no keys, and no official V2L features required.

As the EV market expands, the complexity of its charging infrastructure scales with it. The push for Vehicle-to-Grid (V2G) communication capabilities introduces a significant attack surface with destructive potential for high-voltage systems. In this talk, we explore the security risks within current V2G communication. We break down exactly how this data is processed internally, map out the high-voltage charging architecture, and expose logic weaknesses hiding within the vehicle's Battery Management System (BMS) ECUs.

Based on this research, we introduce ChargeSploit, a custom hardware and software toolkit designed for cybersecurity testing of the EV charging ecosystem. Capable of simulating both vehicles and chargers, or acting as a physical Man-in-the-Middle, ChargeSploit allows researchers to intercept, manipulate, and inject payloads into live communication flows. We conclude with a live demonstration exploiting V2G protocols and the BMS to force an unauthorized discharge, successfully powering an iPhone directly from a locked EV's traction battery.

Speakers: Fabien Guillebot, Stepan Konicek

SpeakerBio: Fabien Guillebot, Accenture

Fabien Guillebot is a Hardware Security Researcher at Accenture based in Prague, Czech Republic. He specializes in hardware-level security testing with a primary focus on the automotive sector. Fabien's core expertise lies in designing custom hardware for specialized penetration testing and conducting advanced research in microcontroller glitching and fault injection.

SpeakerBio: Stepan Konicek, Accenture

Stepan Konicek, MSc. is an Embedded Systems Penetration Tester at Accenture based in Prague, Czech Republic. Specializing in automotive cybersecurity, Stepan focuses on testing and securing ECUs and full-vehicle architectures. His primary research focus lies in EV charging security, where he investigates the physical and protocol-level vulnerabilities that exist between modern vehicles and grid infrastructure.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Hook Crook - Extracting More From Discord Webhooks

Tags: Intro/Beginner | DEF CON Demo Labs | AppSec | Offense/Red Team | Threat Intel/Hunting | DEF CON Demo Labs

When: Saturday, Aug 8, 13:00 - 13:45 PDT

Where: LVCCW Level 1 Hall 3 900 (Demo Labs Track 4) - [Map](#)

Description:

A webhook URL is often thought to be write-only — post a message, nothing more. So when one leaks through a misconfigured repo, a paste site, or breached infrastructure, it's written off as a spam-or-phishing nuisance and left to rot. Hook Crook shows that assumption is the vulnerability — and that "write-only" was never really the case.

By abusing how Discord resolves references, what it returns when you query users and messages, and how its error and rate-limit responses differ, the write-only token quietly becomes a read primitive — leaking by design, not by bug. With nothing but the URL — no account, no additional authentication, no interaction from anyone on the target server — Hook Crook fingerprints the host guild, enumerates and confirms members, pulls profile data on known users (including their home-server tag), and in some cases recovers message content. The same behaviors let it bypass the server's posting restrictions, stage convincing impersonation and phishing, quietly edit or delete messages to scrub the evidence, and — on the way out — delete the webhook itself. None of it breaks Discord — it just reads Discord more carefully than its designers intended.

Speakers:Jeremy Banker - K0JLB,Arity0

SpeakerBio: Jeremy Banker - K0JLB

Bio: Jeremy Banker is a Senior Security Software Engineer at Horizon3.ai, focused on the reliability and resiliency of Horizon3's automated penetration testing platform. He previously spent nearly a decade at VMware, where he co-founded the Security Product Engineering group and led efforts to secure VMware's software supply chain. His open source security tooling, including Build Inspector for CI/CD pipeline anomaly detection and Tommyknocker for automated security control validation, has been featured at Black Hat Arsenal and DEF CON Demo Labs. A licensed amateur radio operator since 2010, he built open-packet, an MIT licensed Python client for packet messaging, after becoming frustrated with the existing closed-source options.

SpeakerBio: Arity0

Arity0 is an independent security researcher specializing in the Discord platform. A self-taught hacker, he focuses on uncovering undocumented behaviors, edge cases, and design-level privacy implications in Discord's API and rendering pipeline. His long-running exploration of Discord's rendering quirks led to the discovery of the webhook rendering oracles that form the foundation of the Hook Crook identity disclosure technique.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Hook Crook - Extracting More From Discord Webhooks

Tags: Intro/Beginner | DEF CON Demo Labs | AppSec | Offense/Red Team | Threat Intel/Hunting | DEF CON Demo Labs

When: Saturday, Aug 8, 14:00 - 14:45 PDT

Where: LVCCW Level 1 Hall 3 900 (Demo Labs Track 4) - [Map](#)

Description:

A webhook URL is often thought to be write-only — post a message, nothing more. So when one leaks through a misconfigured repo, a paste site, or breached infrastructure, it's written off as a spam-or-phishing nuisance and left to rot. Hook Crook shows that assumption is the vulnerability — and that "write-only" was never really the case.

By abusing how Discord resolves references, what it returns when you query users and messages, and how its error and rate-limit responses differ, the write-only token quietly becomes a read primitive — leaking by design, not by bug. With nothing but the URL — no account, no additional authentication, no interaction from anyone on the target server — Hook Crook fingerprints the host guild, enumerates and confirms members, pulls profile data on known users (including their home-server tag), and in some cases recovers message content. The same behaviors let it bypass the server's posting restrictions, stage convincing impersonation and phishing, quietly edit or delete messages to scrub the evidence, and — on the way out — delete the webhook itself. None of it breaks Discord — it just reads Discord more carefully than its designers intended.

Speakers:Jeremy Banker - K0JLB,Arity0

SpeakerBio: Jeremy Banker - K0JLB

Bio: Jeremy Banker is a Senior Security Software Engineer at Horizon3.ai, focused on the reliability and resiliency of Horizon3's automated penetration testing platform. He previously spent nearly a decade at VMware, where he co-founded the Security Product Engineering group and led efforts to secure VMware's software supply chain. His open source security tooling, including Build Inspector for CI/CD pipeline anomaly detection and Tommyknocker for automated security control validation, has been featured at Black Hat Arsenal and DEF CON Demo Labs. A licensed amateur radio operator since 2010, he built open-packet, an MIT licensed Python client for packet messaging, after becoming frustrated with the existing closed-source options.

SpeakerBio: Arity0

Arity0 is an independent security researcher specializing in the Discord platform. A self-taught hacker, he focuses on uncovering undocumented behaviors, edge cases, and design-level privacy implications in Discord's API and rendering pipeline. His long-running exploration of Discord's rendering quirks led to the discovery of the webhook rendering oracles that form the foundation of the Hook Crook identity disclosure technique.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Hook, Line & Pretext Workshop: Crafting Effective Phish

Tags: Social Engineering Community Village | Creator Event/Activity

When: Saturday, Aug 8, 13:30 - 14:59 PDT

Where: LVCCW Level 3 W320 (Social Engineering Community Village Labs) - [Map](#)

Description:

Every effective phishing email is really a marketing email with a hostile goal. It wins attention, builds desire, and drives a single click. This hands-on introductory workshop pulls back the curtain on that craft. In 90 minutes you'll learn the persuasion techniques that make a lure irresistible, borrowed straight from the sales and marketing playbook: the handful of influence levers that actually move people, the copywriting structure behind a high-converting message, and the emotional triggers that turn a glance into a click. Then you'll add the ingredient that separates a generic blast from a believable one, which is context, using open-source intelligence (OSINT) to tie a lure to a real department, location, or current event so it feels timely and true. You won't just watch. After we run the full method end to end against a familiar fictional target, the Scranton branch of Dunder Mifflin, you'll roll up your sleeves and build your own department or location wide pretext against a real organization you know. You'll walk out able to reason about why people click, not just that they do, with a repeatable process and a finished lure you can take straight back to your own awareness program. This is a content-creation and analysis workshop. No live phishing is conducted and no email is ever sent. Who it's for: Aspiring and early-career security practitioners, security-awareness and blue-team staff who want to think like an attacker, IT professionals moving toward security, and students or career-changers exploring offensive security. Anyone who builds or improves a phishing-awareness program will get direct, practical value. Level and prerequisites: Introductory. No prior phishing, red-team, or OSINT experience required. You should be comfortable using a web browser and reading professional email. Nothing to install, no coding, no command line. What to bring ' A laptop with a web browser, for light open-source research during the lab ' A real organization you know: your employer, your school or university, a nonprofit or club you belong to, or a former workplace, etc. ' Something to write with. All worksheets are provided ' Curiosity and a willingness to share your draft for friendly peer feedback What you'll leave with ' The three-gates test (legality, then ethics, then morality) for vetting any campaign before it runs ' A working command of the four influence levers that drive clicks and the "one hook, one ask, one button" rule for writing them ' A repeatable OSINT-to-pretext method for making lures timely and relevant to a department or location ' A completed Pretext Canvas and a draft, awareness-grade phishing email you can optionally submit to your own organization's security-awareness program Format and duration: A hands-on 90 minutes: about 30 minutes of instruction, a 10-minute guided case study against Dunder Mifflin, and roughly 50 minutes of lab with peer review and debrief. What this workshop is not: It's not a tooling or infrastructure course. There are no phishing frameworks, payloads, landing pages, or email spoofing. It's not spear-phishing of named individuals; the focus is wide-net, department and location-level pretexts. And nothing is ever sent.

Speakers:Jenn,JC

SpeakerBio: Jenn

Jenn (@_nextjenn) is a Senior Offensive Security Consultant and a DEF CON Black Badge holder, earned by winning the vishing competition. With over a decade of cybersecurity experience, she specializes in social engineering, physical security testing, and network penetration testing. Leveraging her background in psychology and experience as a licensed Private Investigator and Locksmith, she has led sophisticated red team engagements across physical penetration testing, phishing, vishing, and deepfake-driven operations. An active mentor and coach in the social engineering community, Jenn has judged DEF CON's 2024 "Humans vs AI" and 2025 Vishing competitions and shares insights through podcasts and conference talks, including Wild West Hackin' Fest and San Diego Comic-Con.

SpeakerBio: JC, President at Snowfensive

JC is a U.S. Marine Corps veteran, President of Snowfensive, and co-founder of the Social Engineering Community Village at DEF CON. With more than a decade of experience spanning information technology, digital forensics, incident response,

penetration testing, and social engineering, he specializes in turning complex security concepts into practical skills people can immediately apply.

At Snowfensive, JC oversees the company's offensive security services, including phishing, vishing, physical social engineering, covert entry assessments, and technical penetration testing across networks, wireless environments, and applications. He has designed and led human-focused security engagements for organizations across a wide range of industries, combining technical tradecraft with a practical understanding of how people, processes, and technology intersect.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Hostile Input: PDF Triage That Survives an Adversarial Document

Tags: Malware Village | Creator Workshop

When: Saturday, Aug 8, 10:10 - 12:10 PDT

Where: LVCCW Level 1 Hall 2 600 (Malware Village) Workshops - [Map](#)

Description:

Abstract A malicious document is no longer only a payload for the endpoint. It is an input your tooling has to parse and judge, and as SOC teams bolt language models onto triage, that input becomes something an attacker can shape to corrupt the verdict itself. This workshop treats the document as an adversarial surface aimed at the analyst's tooling, including the analyst's AI.

It is hands-on, starting from basic command-line tools, participants build the techniques that defeat AI-assisted triage, then build triage that survives them: a prompt injection placed where no human reader sees it, a metadata and ToUnicode parser differential where the renderer and the extractor disagree on the same glyphs, and a staged payload the document never reveals on its own. The two contributions that carry the workshop are treating extractor disagreement as a detection signal, and a triage architecture where a deterministic stage owns the verdict and the model is confined to advisory roles downstream of it.

Participants leave with a working pipeline, the sample set, and a scoring harness, and can state exactly where a language model belongs in triage and why putting it anywhere else is the vulnerability. The pipeline runs locally on modest models, because the detection power is in the tooling, not the model. Clean files never leave the environment.

Outline Deterministic floor. Point an autonomous agent at a file, watch an indirect injection in the document hijack it. That failure is the problem statement. Participants then lay the structural floor with pdfid and pdf-parser: the facts an attacker cannot phrase their way out of.

Demote the model. Analyze a malicious PDF structurally, then watch a hidden render-mode injection talk a naive model pipeline into a clean verdict. Rebuild it so a deterministic stage owns the verdict and the model is fed structural findings, not the attacker's prose. Rule: extracted content is untrusted input, never instruction.

Add redundancy: the parser differential. Two documents that defeat detection by placement alone: an injection living in metadata a body-text extractor never reads, a ToUnicode trick that makes the rendered page and the extracted text disagree on identical glyphs. Participants build a multi-extractor differential and treat disagreement as the alert.

Resolve, and place the model. A staged payload forces the last lesson: Participants add input validation and type-confusion detection at the floor, extract the hidden artefact as a suspicion finding, decode it in-terminal, and let bounded model roles explain it and assemble competing hypotheses with evidence while the analyst decides. The model advises downstream of a deterministic gate, never holds the verdict.

Capstone CTF and Q&A. A fresh set: technique-carriers, clean decoys, and documents styled as benign PDFs that baits the analyst into pasting it straight into the model. Participants show their work: verdict, technique, extraction path, hidden URLs, execution behaviour. Scoring rewards correctness first, then fewest tokens, because the analyst who needed the model least played the strongest game.

Learning objectives Participants will be able to: 1. Build a PDF triage pipeline from command-line tools and explain exactly where its verdict comes from. 2. Analyze a malicious PDF structurally (pdfid, pdf-parser, stream inspection) and decode embedded artefacts in-terminal. 3. Construct and recognize the three adversarial-document techniques that defeat AI-assisted analysis: hidden-layer prompt injection, metadata and ToUnicode parser differentials, and staged payloads. 4. Distinguish an early structural suspicion verdict from a late analytical identification verdict, and treat extractor disagreement as a detection signal. 5. Place a language model in bounded advisory roles downstream of a deterministic gate, never holding the verdict, and select the right model for each task. 6. Run the whole pipeline locally on modest models, understanding why the detection power lives in the tooling and why the architecture is private by construction.

SpeakerBio: Klaus Wunder, Principal Cyber Defence Analyst at SECUINFRA

With nearly two decades in cybersecurity, Klaus has gone from configuring firewalls to protecting industrial control systems where breaches cost safety, not just data. That journey gives him a full-spectrum perspective on security operations. He guides teams through complex incidents and builds detection engineering capabilities across hybrid environments as a Principal Cyber Defence Analyst, while his role as an Authorized OffSec Instructor, Ambassador keeps him equally focused on developing the next generation of analysts. His current work explores how Large Language Models can revolutionize cyber defence with practical applications, not hype. He recently launched The Analyst Mind on Substack (theanalystmind.io), where he writes about analytical thinking, critical frameworks, and the evolving analyst mindset.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: How Malicious AI Skills Hijack Your Agents

Tags: Intermediate | AppSec Village | Creator Talk/Panel

When: Saturday, Aug 8, 15:30 - 15:59 PDT

Where: LVCCW Level 1 Hall 2 604 (Appsec Village) Main Stage - [Map](#)

Description:

When OpenClaw went viral in January 2026, threat actors were in ClawHub within hours. They didn't need to exploit a vulnerability - they just opened a GitHub account and uploaded malicious AI skills. Within weeks, over 700 malicious skills had shipped, all designed to steal crypto and credentials from unsuspecting users. When maintainers added scanning, attackers moved their payloads off the platform entirely. The green badge stayed green. The malware kept spreading.

This talk uses that campaign as a case study to examine how AI skills get weaponized, why the security signals on skill registries create a false sense of safety, and what practitioners and security leaders can do to evaluate skills safely before installing them.

SpeakerBio: Jenn Gile

Jenn Gile is a community builder and tech educator in the Security and DevOps fields. She's Co-Founder of OpenSourceMalware.com and runs the community program for BSides Seattle. Jenn previously worked at NGINX, F5, Endor Labs, and the U.S. Department of State. Outside of work, she's deeply involved in the cycling community as a board member for 2nd Cycle.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: How much of our Bluetooth firmware reverse engineering work can now be automated with LLMs?

Tags: DEF CON Official Talk | Demo | Tool

When: Saturday, Aug 8, 16:30 - 17:30 PDT

Where: LVCCW Level 1 Hall 3 1007 (Main Track 2) - [Map](#)

Description:

Last year Xeno manually reverse-engineered Realtek RTL8761B* Bluetooth chips' ROM & firmware, to inject code into them that allows everyone to send custom packets that aren't supposed to be possible on a well-behaved device. Previous to that Veronica manually reverse-engineered multiple firmwares to find link layer over-the-air exploitable vulnerabilities. This year we wanted to understand how much time we could have saved on past projects if we had used LLMs to automate the reversing process.

The answer turns out to be "quite a lot!". In this talk we'll discuss how we've created skills for LLMs to almost entirely automate the reverse engineering of Bluetooth Low Energy / Classic chip firmwares' low level packet handling & Host Controller Interface layers. The key is to focus on helping the LLMs find the code that you know *must* be there in order for a chip to be spec-compliant ("Waypoints").

If you work in another firmware/OS RE domain, with well-defined specification-required interfaces and data structures, we expect you'll be able to follow the same process as us to significantly accelerate your reversing. Especially if you have binaries that you've already reverse-engineered in the past that you can feed into an automation process for grading purposes.

[1] "Reverse engineering Realtek RTL8761B* Bluetooth chips, to make better Bluetooth security tools & classes" - Xeno Kovah - <https://darkmentor.com/publication/2025-11-hardweario/>

[2] "DarkFirmware_real_i" - Xeno Kovah - https://github.com/darkmentorllc/DarkFirmware_real_i [3]

Speakers: Veronica Kovah, Xeno Kovah

SpeakerBio: Veronica Kovah, Dark Mentor LLC

Veronica is a researcher who has created and released multiple over-the-air arbitrary code execution exploits which target Bluetooth chip firmware. She presented these attacks at BlackHat USA 2020. In 2018 she founded the security consultancy Dark Mentor LLC. She has previously worked at companies like Tesla on vehicular security and NSA as an adjunct instructor and Capability Development Specialist developing CNE tools for embedded systems. She is currently using her background in reverse engineering and exploitation to specialize in the security analysis of Bluetooth systems.

SpeakerBio: Xeno Kovah, Dark Mentor LLC

Prior to working full time on OpenSecurityTraining2 (ost2.fyi), Xeno worked at Apple designing architectural support for firmware security; and code auditing firmware security implementations. A lot of what he did revolved around adding secure boot support to the main and peripheral processors (e.g. the Broadcom Bluetooth chip.) He led the efforts to bring secure boot to Macs, first with T2-based Macs, and then with the massive architectural change of Apple Silicon Macs. Once the M1 Macs shipped, he left Apple to pursue the project he felt would be most impactful: creating free deep-technical online training material and growing the newly created OpenSecurityTraining 501(c)(3) nonprofit.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: How Shadow APIs Become an Attacker's Free Pass Into Your Cloud-Native App

Tags: Intermediate | AppSec Village | Creator Talk/Panel

When: Saturday, Aug 8, 13:30 - 13:59 PDT

Where: LVCCW Level 1 Hall 2 604 (Appsec Village) Main Stage - [Map](#)

Description:

Old endpoints rarely die. They get forgotten. They survive refactors, go-lives, and cloud migrations, quietly drifting outside the visibility of gateway security testing. Many are inherited through third-party SDKs, shared libraries, and open-source middleware that teams never provisioned and never fully tracked. Built from a real security review of a production mobile app, this talk shows how a legacy authentication endpoint quietly bypassed every modern control around it. Through a live demonstration using only open-source tooling, we show how forgotten APIs can become full paths to compromise and why cloud-native visibility models fail by design.

Speakers: Emma Yuan Fang, Krity

SpeakerBio: Emma Yuan Fang

Emma is a seasoned Security Architect specialising in cloud security and AppSec. As Regional Practice Lead at EPAM, she leads a team of security practitioners across the UK&I, Switzerland, and Germany. Her focus has recently expanded into the intersection of LLMs, MCP, and security, exploring how agentic AI systems reshape the threat landscape. Beyond her day job, Emma is an award-winning conference speaker, a dedicated mentor, and Vice President of WiCyS UK&I, where she champions diversity in the cyber workforce.

SpeakerBio: Krity

Krity is a dedicated cybersecurity professional with a strong foundation in application security, data analysis, and machine learning. As an Application Security Engineer at ServiceNow, she leverages her diverse experience and research background to enhance security practices. Beyond her technical role, Krity serves as the Community & Development Lead at Breaking Barriers Women in Cybersecurity (BBWIC), a nonprofit dedicated to empowering women in the field. Her work reflects a deep commitment to both advancing cybersecurity and fostering inclusive community growth, making her a passionate advocate for innovation, collaboration, and leadership in the industry.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Malware Village - Saturday - 13:50-14:30 PDT

Title: How to destroy a country

Tags: Malware Village | Creator Talk/Panel

When: Saturday, Aug 8, 13:50 - 14:30 PDT

Where: LVCCW Level 1 Hall 2 600 (Malware Village) Talks - [Map](#)

Description:

Some people just want to see the whole world burn. And some cyberwarfare units just want your systems to go *puff*.

Wipers are the cyber version of napalm, taking destruction from the kinetic to the cyberspace, and have been the most utilized weapons by cyberwars in the last decade. These wipers are design to destroy everything that they can get their hands on to: files, disks, backups, you name it. And they are purposefully designed this way by a dedicated group with their destabilizing a whole country in times of war.

In this talk we are going to go through the history of wipers, since our discovery of Flame in 2012 to our latest research on a destructive wiper we named Lotus Wiper. We are going to go through the technical details as well as providing a panoramic view to the impact that these types of cyberweapons have on countries, companies and people around the globe.

Speakers: Lisandro Ubiedo, Leandro Cuzzo

SpeakerBio: Lisandro Ubiedo, Senior Security Researcher at Kaspersky GReAT LATAM

Lisandro is currently a security researcher, part of the GReAT team at Kaspersky. Previously, he was part of the security research team at GoSecure and collaborator at Stratosphere Labs based on Czech Republic. He's focused on analyzing and tracking threat actors in Latin America, creating profiles and reporting on their doings.

SpeakerBio: Leandro Cuzzo, Cybersecurity investigator at Kaspersky

Investigador de Seguridad en el equipo GReAT de Kaspersky. Cuento con más de 12 años de experiencia en ciberseguridad. Ex mantenedor principal de la suite Impacket.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Payment Village - Friday - 14:00-14:45 PDT

Title: How to Epically Fail Your PCI Assessment

Tags: Payment Village | Creator Talk/Panel

When: Friday, Aug 7, 14:00 - 14:45 PDT

Where: LVCCW Level 2 W204-205 (Payment Village) - [Map](#)

Description:

If your company accepts, processes, stores, transmits, dreams about, or accidentally leaves cardholder data on a sticky note, congratulations - you get the privilege of dealing with PCI DSS. For organizations processing enough transactions, the reward for your success is an on-site assessment conducted by a Qualified Security Assessor (QSA). Think of it as inviting a well-dressed, highly trained auditor to examine every corner of your security program and ask uncomfortable questions about decisions made by people who left the company three years ago.

In an ideal world, your controls are well-documented, operating effectively and everyone knows exactly where the evidence is stored. In the real world, someone discovers during the assessment that the quarterly review hasn't happened since the last presidential administration, nobody can explain a firewall rule labeled "DO NOT TOUCH" and a frantic war room appears overnight.

This session explores the most common (and a few impressively creative) ways organizations derail their PCI assessments. We'll cover how to avoid discovering critical compliance gaps in front of your QSA, why "we thought someone else was doing that" is not a valid control and how to prevent your assessment from turning into a high-stakes race against the reporting deadline.

Come learn how not to fail your PCI assessment spectacularly... preferably before your next assessment cycle.

SpeakerBio: Kevin Buck, PCI GRC Manager, NBCUniversal

40+ years in technology across roles from system programmer to CTO; involved in PCI compliance since 2005 as both a Level 1 merchant and a Qualified Security Assessor (QSA).

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Hackers.town - Saturday - 11:00-11:59 PDT

Title: How to get RCE on a car

Tags: Hackers.town | Creator Talk/Panel

When: Saturday, Aug 8, 11:00 - 11:59 PDT

Where: LVCCW Level 1 Hall 4 1420 (Hackers.town) - [Map](#)

Description:

SpeakerBio: Ac0rn

No BIO available



[Return to Index](#) - Add to Google

- ics [Calendar](#) file

Title: How to piss off your Nix friends

Tags: Nix Vegas Community | Creator Talk/Panel

When: Saturday, Aug 8, 10:30 - 10:45 PDT

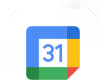
Where: LVCCW Level 1 Hall 4 1310 (Nix Vegas Community) - [Map](#)

Description:

Nix is surging in popularity, and with it the community has taken the stance that Nix should be for everyone & their grandparents. I'm here to fight against that idea and share why I think it dilutes the power of Nix itself. By catering to the masses and targeting multiple platforms (MacOS), we weaken the potential of the idea and implementation. When we stop building for the lowest common denominator, we get to push the absolute limits. I will spend this time trying to convince you why Nix should drop support for platforms such as MacOS, diverge even more radically from traditional Linux distros and take on more grand technical solutions to problems at large.

SpeakerBio: Farid Zakaria

I'm a software engineer, father and wishful amateur surfer. If you've come seeking my political views, you've found the wrong. You can find my writings on Nix, build systems and software engineering in general at <https://fzakaria.com>



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: How to Profile an entire C-suite in 10 days

Tags: OSINT For Good Community | Creator Talk/Panel

When: Sunday, Aug 9, 10:30 - 10:59 PDT

Where: LVCCW Level 1 Hall 4 1307 (OSINT4Good Community) Stage - [Map](#)

Description:

How long do you think it takes to find sensitive information on the executives of a major company? It is sometimes wrongly believed that VIPs have better digital hygiene than us regular humans, that their information is not present on any people search site, and that their dubious online past has been wiped from the internet. This is false. Throughout this talk I will show you how I approach a vulnerability assessment on the c-suite of a multinational corporation. From the boring stuff like note taking and report writing, to the really exciting stuff like wacky sources and fun findings.

SpeakerBio: Sarah Muriel, Bishop Fox

Sarah Muriel is an Intelligence Analyst from Mexico with more than 6 years of experience in open source investigations, currently working with the Attack Surfaces of companies all over the world. In her spare time she likes participating in various international OSINT related CTFs and developing retro-style websites. She's also fairly active in the cybersecurity community, being part of the organization team for one of Mexico's top conferences.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Bug Bounty Village - Sunday - 12:00-12:59 PDT

Title: How We Built Xenoptic: A Walkthrough of Design, Infrastructure and Vulns!

Tags: Bug Bounty Village | Creator Talk/Panel

When: Sunday, Aug 9, 12:00 - 12:59 PDT

Where: LVCCW Level 2 W206-207 (Bug Bounty Village) - [Map](#)

Description:

In this talk, the CTF.ae team goes behind the scenes of Xenoptic: how they built this year's BBV CTF lab, the new challenges they hit along the way, and a walkthrough of some of the most interesting vulnerabilities they planted in it.

Speakers: Adham Elmosalamy, Ahmed Attalla, Yousef Awad, Kasimir Schulz

SpeakerBio: Adham Elmosalamy, Security Researcher, CTF.ae

Adham is an offensive security consultant by day, but when the sun sets he returns to what he enjoys most: CTFs. This year he led the team building Xenoptic, working across application security, UI/UX and game balance.

SpeakerBio: Ahmed Attalla, Founder, CTF.ae

I run <https://ctf.ae/>

SpeakerBio: Yousef Awad

No BIO available

SpeakerBio: Kasimir Schulz

No BIO available

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Contests - Saturday - 10:00-17:59 PDT

Title: HSPACE: AI Battlegrounds

Tags: HSPACE: AI Battlegrounds | Contest

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 205 (HSPACE: AI Battlegrounds) - [Map](#)

Description:

"Your prompt becomes a character, a machine, or an attack—and every word can change what happens next.

HSPACE: AI Battlegrounds is a collection of three hands-on games that turn natural-language and visual prompts into playable systems:

Wizard of Prompts — Write a short prompt to generate a pixel-art hero with unique stats and skills, then guide that hero through a five-boss, card-based battle campaign. Experiment with wording, build a stronger character, and see how the game's AI responds to prompt-injection attempts.

Prompt Prix — Describe your ideal race car and watch the AI convert your prompt into a validated vehicle build. Race across changing track conditions, study the result, and tune your prompt to improve the car's speed, grip, stability, and final ranking.

Vision Breaker — Face a vision-language-model security guard that decides who may enter. Use signs, screens, clothing, props, and visual prompt-injection techniques to influence its observations, bypass its checks, and progress through three escalating stages—from changing a decision to hijacking a command.

No joystick, coding experience, or prior security knowledge is required. Come experiment, iterate, and discover how small changes in language and visual context can reshape an AI agent's behavior.

Participant Prerequisites

Anyone who has used AI at least once is welcome. A camera-enabled smartphone or laptop with a modern web browser is recommended for Vision Breaker; camera permission is required for live play. Game stations and physical props are provided at the booth.

Participants can also play on their own smartphones or personal laptops. The competitive portion of AI Battlegrounds will be conducted online."

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: HSPACE: AI Battlegrounds

Tags: HSPACE: AI Battlegrounds | Contest

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 205 (HSPACE: AI Battlegrounds) - [Map](#)

Description:

"Your prompt becomes a character, a machine, or an attack—and every word can change what happens next.

HSPACE: AI Battlegrounds is a collection of three hands-on games that turn natural-language and visual prompts into playable systems:

Wizard of Prompts — Write a short prompt to generate a pixel-art hero with unique stats and skills, then guide that hero through a five-boss, card-based battle campaign. Experiment with wording, build a stronger character, and see how the game's AI responds to prompt-injection attempts.

Prompt Prix — Describe your ideal race car and watch the AI convert your prompt into a validated vehicle build. Race across changing track conditions, study the result, and tune your prompt to improve the car's speed, grip, stability, and final ranking.

Vision Breaker — Face a vision-language-model security guard that decides who may enter. Use signs, screens, clothing, props, and visual prompt-injection techniques to influence its observations, bypass its checks, and progress through three escalating stages—from changing a decision to hijacking a command.

No joystick, coding experience, or prior security knowledge is required. Come experiment, iterate, and discover how small changes in language and visual context can reshape an AI agent's behavior.

Participant Prerequisites

Anyone who has used AI at least once is welcome. A camera-enabled smartphone or laptop with a modern web browser is recommended for Vision Breaker; camera permission is required for live play. Game stations and physical props are provided at the booth.

Participants can also play on their own smartphones or personal laptops. The competitive portion of AI Battlegrounds will be conducted online."

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: HSPACE: AI Battlegrounds

Tags: HSPACE: AI Battlegrounds | Contest

When: Sunday, Aug 9, 10:00 - 11:59 PDT

Where: LVCCW Level 1 Hall 1 205 (HSPACE: AI Battlegrounds) - [Map](#)

Description:

"Your prompt becomes a character, a machine, or an attack—and every word can change what happens next.

HSPACE: AI Battlegrounds is a collection of three hands-on games that turn natural-language and visual prompts into playable systems:

Wizard of Prompts — Write a short prompt to generate a pixel-art hero with unique stats and skills, then guide that hero through a five-boss, card-based battle campaign. Experiment with wording, build a stronger character, and see how the game's AI responds to prompt-injection attempts.

Prompt Prix — Describe your ideal race car and watch the AI convert your prompt into a validated vehicle build. Race across changing track conditions, study the result, and tune your prompt to improve the car's speed, grip, stability, and final ranking.

Vision Breaker — Face a vision-language-model security guard that decides who may enter. Use signs, screens, clothing, props, and visual prompt-injection techniques to influence its observations, bypass its checks, and progress through three escalating stages—from changing a decision to hijacking a command.

No joystick, coding experience, or prior security knowledge is required. Come experiment, iterate, and discover how small changes in language and visual context can reshape an AI agent's behavior.

Participant Prerequisites

Anyone who has used AI at least once is welcome. A camera-enabled smartphone or laptop with a modern web browser is recommended for Vision Breaker; camera permission is required for live play. Game stations and physical props are provided at the booth.

Participants can also play on their own smartphones or personal laptops. The competitive portion of AI Battlegrounds will be conducted online."

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Human in the Loop or Human Out of Luck?

Tags: Biohacking Village | Creator Talk/Panel

When: Friday, Aug 7, 11:30 - 11:59 PDT

Where: LVCCW Level 1 Hall 3 1104 (Creator Stage 4) - [Map](#)

Description:

As agentic AI systems rapidly enter healthcare and precision medicine, a critical question remains largely unanswered: what happens when the patient is reduced to data alone? This talk explores a real-world experiment conducted through GENE240 at Stanford, where interdisciplinary student teams used agentic AI systems and multiomic datasets to investigate a complex patient case. Working across genomics, computational biology, and clinical reasoning, teams analyzed the same underlying data while arriving at dramatically different hypotheses, interpretations, and priorities. Unlike traditional case studies, the patient was actively involved throughout the process. While full medical records were intentionally withheld, selective contextual information and direct interaction with the patient significantly influenced the direction and interpretation of the work. The experience exposed both the extraordinary promise and the profound limitations of AI-driven healthcare systems. This session will examine: how agentic AI systems behave when operating on incomplete clinical context the variability introduced by tooling, prompting, and disciplinary bias the role of patient interaction in refining computational hypotheses why lived experience may be one of the most underutilized datasets in precision medicine Through the lens of rare disease and complex chronic illness, this talk challenges the assumption that more data alone leads to better outcomes. Instead, it argues that the future of AI-enabled healthcare depends on keeping patients actively embedded in the interpretive loop. For the biohacking community, this raises broader questions around autonomy, data ownership, participatory medicine, and how individuals may increasingly interface with AI systems to investigate their own health outside traditional clinical

SpeakerBio: Christine Von Raesfeld

Christine is a research advocate and community engagement leader focused on health, data, and emerging technologies. Living with multiple rare and chronic conditions, she advances participatory medicine and champions people with lived experience as essential partners in research and innovation.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Human Registration Open

Tags: Misc

When: Saturday, Aug 8, 09:00 - 18:59 PDT

Where: LVCC West Hall

Description:

Our human registration process this year will be very similar to previous years. Please be patient. All of the times listed here are **approximate**.

Basics

Who needs a badge?

A badge is required for each human age 8 and older.

Human?

You are a human if you do not know otherwise. People that are not humans include goons, official speaker, village/community/contest/creator staff, press, black badge holders, or similar. If you are not a human, you need to register separately. If you don't know how, see an NFO goon (NFO Node, formerly known as an infobooth, is where you can get help). The remainder of this message applies only to humans.

Lines? Linecon?

Linecon is your optional opportunity to stand (or sit) in line for human registration to open. Doors will open for linecon on Wednesday at approximately 17:00. When human registration opens on Thursday at approximately 08:00, they start working the linecon queue, and the line will start moving quickly. (Please understand that we will begin processing the line on Thursday morning as soon as the cashiers and materials are in place; we will strive for Thursday 08:00, but actual start may be slightly earlier or later.)

Online badge purchase (aka pre-registration) has no impact on linecon. You can join the line on Wednesday (if you wish) regardless of whether you purchased a badge online or intend to pay with cash. There is only one linecon for both types of badge sales.

Please help us make this a great experience for everyone by **following directions given by goons**. After human registration opens, there may be one line for all of registration, or there may be two lines (one for online sales (pre-registration) and one for cash sales). This may also change over time, based on available staffing and necessary crowd control. We will strive to make it easily understandable in-person as to which line you should join.

Ways to buy a badge

- \$560-600 [online purchase](#) until August 1, 2026. Tickets are transferable. Please read the details on the linked page.
- \$520 cash purchase on-site.
- As part of a BlackHat registration.

Online Purchase

You will be emailed a QR code to the email address provided when you bought your badge. Please guard that QR code as though it is cash -- it can only be redeemed once, and anyone can redeem it if they have it (including a photo of it). Badges are picked-up on-site -- they will not be mailed or shipped.

We can scan the QR code either from your phone's display or from a printed copy. You **must** have the QR code with you in order to obtain your badge. As you approach the front of the line, if you are going to show your QR code on an electronic device, please ensure that your display is set to maximum brightness.

If you pre-registered, but ultimately are unable to attend DEF CON and want to cancel your purchase, the **only** way to get a refund is from the original online source. We are unable to provide any refunds on-site at DEF CON. There is a fee to have your badge canceled: \$34 before July 18, and \$84 on and after July 18.

Online purchases are provided a receipt via email when the purchase is made.

Online purchase -- often referred to as pre-registration -- does not allow you to skip any line/queue to pick up your badge. Once you arrive on-site, you will need to join the existing line for human registration. There may or may not be a dedicated line for pre-registration badge pickup, depending on when you arrive, how long the line is, available staff, etc.

Cash Purchase

Badges will be available for purchase on-site at DEF CON. All badge sales are **cash only**. No checks, money orders, credit cards, etc., will be accepted. In order to keep the registration line moving as quickly as possible, please have **exact change** ready as you near the front of the line.

There are no refunds given for cash sales. If you have any doubt about your desire to buy a badge, please refrain from doing so.

We are unable to provide printed receipts at the time of the sale. A generic receipt for the cash sale of a badge will be made available on media.defcon.org after the conference. You are welcome to print your own copy of the receipt on plain paper.

Via BlackHat

If you've purchased a DEF CON badge as part of your Black Hat registration, you're in luck - you will be able to pick up your DEF CON badge at Black Hat on Thursday. Please bring your Black Hat badge and watch for emails from Black Hat about where exactly the badge pickup will be.

Please note that DEF CON is not able to access or verify Black Hat registration or attendee info. DEF CON's preregistration list is not the same as Black Hat's. For help, ask at Black Hat registration or the concierge area.

Misc

Want to buy multiple badges? No problem! We're happy to sell you however many badges you want to pay for.

If you lose your badge, there is unfortunately no way for us to replace it. You'll have to buy a replacement at full price. Please don't lose your badge. :(

If you are being accompanied by a full-time caretaker (such as someone who will push your wheelchair, and will accompany you at all times), please ask to speak to a Registration Goon. Your caretaker will receive a paper badge that will permit them to accompany you everywhere you go.

Still need help?

If you have questions about anything regarding human registration that are not addressed here, please ask to speak to a Registration Goon.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Human Registration Open

Tags: Misc

When: Friday, Aug 7, 08:00 - 18:59 PDT

Where: LVCC West Hall

Description:

Our human registration process this year will be very similar to previous years. Please be patient. All of the times listed here are **approximate**.

Basics

Who needs a badge?

A badge is required for each human age 8 and older.

Human?

You are a human if you do not know otherwise. People that are not humans include goons, official speaker, village/community/contest/creator staff, press, black badge holders, or similar. If you are not a human, you need to register separately. If you don't know how, see an NFO goon (NFO Node, formerly known as an infobooth, is where you can get help). The remainder of this message applies only to humans.

Lines? Linecon?

Linecon is your optional opportunity to stand (or sit) in line for human registration to open. Doors will open for linecon on Wednesday at approximately 17:00. When human registration opens on Thursday at approximately 08:00, they start working the linecon queue, and the line will start moving quickly. (Please understand that we will begin processing the line on Thursday morning as soon as the cashiers and materials are in place; we will strive for Thursday 08:00, but actual start may be slightly earlier or later.)

Online badge purchase (aka pre-registration) has no impact on linecon. You can join the line on Wednesday (if you wish) regardless of whether you purchased a badge online or intend to pay with cash. There is only one linecon for both types of badge sales.

Please help us make this a great experience for everyone by **following directions given by goons**. After human registration opens, there may be one line for all of registration, or there may be two lines (one for online sales (pre-registration) and one for cash sales). This may also change over time, based on available staffing and necessary crowd control. We will strive to make it easily understandable in-person as to which line you should join.

Ways to buy a badge

- \$560-600 [online purchase](#) until August 1, 2026. Tickets are transferable. Please read the details on the linked page.
- \$520 cash purchase on-site.
- As part of a BlackHat registration.

Online Purchase

You will be emailed a QR code to the email address provided when you bought your badge. Please guard that QR code as though it is cash -- it can only be redeemed once, and anyone can redeem it if they have it (including a photo of it). Badges are picked-up on-site -- they will not be mailed or shipped.

We can scan the QR code either from your phone's display or from a printed copy. You **must** have the QR code with you in order to obtain your badge. As you approach the front of the line, if you are going to show your QR code on an electronic device, please ensure that your display is set to maximum brightness.

If you pre-registered, but ultimately are unable to attend DEF CON and want to cancel your purchase, the **only** way to get a refund is from the original online source. We are unable to provide any refunds on-site at DEF CON. There is a fee to have your badge canceled: \$34 before July 18, and \$84 on and after July 18.

Online purchases are provided a receipt via email when the purchase is made.

Online purchase -- often referred to as pre-registration -- does not allow you to skip any line/queue to pick up your badge. Once you arrive on-site, you will need to join the existing line for human registration. There may or may not be a dedicated line for pre-registration badge pickup, depending on when you arrive, how long the line is, available staff, etc.

Cash Purchase

Badges will be available for purchase on-site at DEF CON. All badge sales are **cash only**. No checks, money orders, credit cards, etc., will be accepted. In order to keep the registration line moving as quickly as possible, please have **exact change** ready as you near the front of the line.

There are no refunds given for cash sales. If you have any doubt about your desire to buy a badge, please refrain from doing so.

We are unable to provide printed receipts at the time of the sale. A generic receipt for the cash sale of a badge will be made available on media.defcon.org after the conference. You are welcome to print your own copy of the receipt on plain paper.

Via BlackHat

If you've purchased a DEF CON badge as part of your Black Hat registration, you're in luck - you will be able to pick up your DEF CON badge at Black Hat on Thursday. Please bring your Black Hat badge and watch for emails from Black Hat about where exactly the badge pickup will be.

Please note that DEF CON is not able to access or verify Black Hat registration or attendee info. DEF CON's preregistration list is not the same as Black Hat's. For help, ask at Black Hat registration or the concierge area.

Misc

Want to buy multiple badges? No problem! We're happy to sell you however many badges you want to pay for.

If you lose your badge, there is unfortunately no way for us to replace it. You'll have to buy a replacement at full price. Please don't lose your badge. :(

If you are being accompanied by a full-time caretaker (such as someone who will push your wheelchair, and will accompany you at all times), please ask to speak to a Registration Goon. Your caretaker will receive a paper badge that will permit them to accompany you everywhere you go.

Still need help?

If you have questions about anything regarding human registration that are not addressed here, please ask to speak to a Registration Goon.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Human Registration Open

Tags: Misc

When: Sunday, Aug 9, 09:00 - 11:59 PDT

Where: LVCC West Hall

Description:

Our human registration process this year will be very similar to previous years. Please be patient. All of the times listed here are **approximate**.

Basics

Who needs a badge?

A badge is required for each human age 8 and older.

Human?

You are a human if you do not know otherwise. People that are not humans include goons, official speaker, village/community/contest/creator staff, press, black badge holders, or similar. If you are not a human, you need to register separately. If you don't know how, see an NFO goon (NFO Node, formerly known as an infobooth, is where you can get help). The remainder of this message applies only to humans.

Lines? Linecon?

Linecon is your optional opportunity to stand (or sit) in line for human registration to open. Doors will open for linecon on Wednesday at approximately 17:00. When human registration opens on Thursday at approximately 08:00, they start working the linecon queue, and the line will start moving quickly. (Please understand that we will begin processing the line on Thursday morning as soon as the cashiers and materials are in place; we will strive for Thursday 08:00, but actual start may be slightly earlier or later.)

Online badge purchase (aka pre-registration) has no impact on linecon. You can join the line on Wednesday (if you wish) regardless of whether you purchased a badge online or intend to pay with cash. There is only one linecon for both types of badge sales.

Please help us make this a great experience for everyone by **following directions given by goons**. After human registration opens, there may be one line for all of registration, or there may be two lines (one for online sales (pre-registration) and one for cash sales). This may also change over time, based on available staffing and necessary crowd control. We will strive to make it easily understandable in-person as to which line you should join.

Ways to buy a badge

- \$560-600 [online purchase](#) until August 1, 2026. Tickets are transferable. Please read the details on the linked page.
- \$520 cash purchase on-site.
- As part of a BlackHat registration.

Online Purchase

You will be emailed a QR code to the email address provided when you bought your badge. Please guard that QR code as though it is cash -- it can only be redeemed once, and anyone can redeem it if they have it (including a photo of it). Badges are picked-up on-site -- they will not be mailed or shipped.

We can scan the QR code either from your phone's display or from a printed copy. You **must** have the QR code with you in order to obtain your badge. As you approach the front of the line, if you are going to show your QR code on an electronic device, please ensure that your display is set to maximum brightness.

If you pre-registered, but ultimately are unable to attend DEF CON and want to cancel your purchase, the **only** way to get a refund is from the original online source. We are unable to provide any refunds on-site at DEF CON. There is a fee to have your badge canceled: \$34 before July 18, and \$84 on and after July 18.

Online purchases are provided a receipt via email when the purchase is made.

Online purchase -- often referred to as pre-registration -- does not allow you to skip any line/queue to pick up your badge. Once you arrive on-site, you will need to join the existing line for human registration. There may or may not be a dedicated line for pre-registration badge pickup, depending on when you arrive, how long the line is, available staff, etc.

Cash Purchase

Badges will be available for purchase on-site at DEF CON. All badge sales are **cash only**. No checks, money orders, credit cards, etc., will be accepted. In order to keep the registration line moving as quickly as possible, please have **exact change** ready as you near the front of the line.

There are no refunds given for cash sales. If you have any doubt about your desire to buy a badge, please refrain from doing so.

We are unable to provide printed receipts at the time of the sale. A generic receipt for the cash sale of a badge will be made available on media.defcon.org after the conference. You are welcome to print your own copy of the receipt on plain paper.

Via BlackHat

If you've purchased a DEF CON badge as part of your Black Hat registration, you're in luck - you will be able to pick up your DEF CON badge at Black Hat on Thursday. Please bring your Black Hat badge and watch for emails from Black Hat about where exactly the badge pickup will be.

Please note that DEF CON is not able to access or verify Black Hat registration or attendee info. DEF CON's preregistration list is not the same as Black Hat's. For help, ask at Black Hat registration or the concierge area.

Misc

Want to buy multiple badges? No problem! We're happy to sell you however many badges you want to pay for.

If you lose your badge, there is unfortunately no way for us to replace it. You'll have to buy a replacement at full price. Please don't lose your badge. :(

If you are being accompanied by a full-time caretaker (such as someone who will push your wheelchair, and will accompany you at all times), please ask to speak to a Registration Goon. Your caretaker will receive a paper badge that will permit them to accompany you everywhere you go.

Still need help?

If you have questions about anything regarding human registration that are not addressed here, please ask to speak to a Registration Goon.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Human Registration Open

Tags: Misc

When: Thursday, Aug 6, 08:00 - 18:59 PDT

Where: LVCC West Hall

Description:

Our human registration process this year will be very similar to previous years. Please be patient. All of the times listed here are **approximate**.

Basics

Who needs a badge?

A badge is required for each human age 8 and older.

Human?

You are a human if you do not know otherwise. People that are not humans include goons, official speaker, village/community/contest/creator staff, press, black badge holders, or similar. If you are not a human, you need to register separately. If you don't know how, see an NFO goon (NFO Node, formerly known as an infobooth, is where you can get help). The remainder of this message applies only to humans.

Lines? Linecon?

Linecon is your optional opportunity to stand (or sit) in line for human registration to open. Doors will open for linecon on Wednesday at approximately 17:00. When human registration opens on Thursday at approximately 08:00, they start working the linecon queue, and the line will start moving quickly. (Please understand that we will begin processing the line on Thursday morning as soon as the cashiers and materials are in place; we will strive for Thursday 08:00, but actual start may be slightly earlier or later.)

Online badge purchase (aka pre-registration) has no impact on linecon. You can join the line on Wednesday (if you wish) regardless of whether you purchased a badge online or intend to pay with cash. There is only one linecon for both types of badge sales.

Please help us make this a great experience for everyone by **following directions given by goons**. After human registration opens, there may be one line for all of registration, or there may be two lines (one for online sales (pre-registration) and one for cash sales). This may also change over time, based on available staffing and necessary crowd control. We will strive to make it easily understandable in-person as to which line you should join.

Ways to buy a badge

- \$560-600 [online purchase](#) until August 1, 2026. Tickets are transferable. Please read the details on the linked page.
- \$520 cash purchase on-site.
- As part of a BlackHat registration.

Online Purchase

You will be emailed a QR code to the email address provided when you bought your badge. Please guard that QR code as though it is cash -- it can only be redeemed once, and anyone can redeem it if they have it (including a photo of it). Badges are picked-up on-site -- they will not be mailed or shipped.

We can scan the QR code either from your phone's display or from a printed copy. You **must** have the QR code with you in order to obtain your badge. As you approach the front of the line, if you are going to show your QR code on an electronic device, please ensure that your display is set to maximum brightness.

If you pre-registered, but ultimately are unable to attend DEF CON and want to cancel your purchase, the **only** way to get a refund is from the original online source. We are unable to provide any refunds on-site at DEF CON. There is a fee to have your badge canceled: \$34 before July 18, and \$84 on and after July 18.

Online purchases are provided a receipt via email when the purchase is made.

Online purchase -- often referred to as pre-registration -- does not allow you to skip any line/queue to pick up your badge. Once you arrive on-site, you will need to join the existing line for human registration. There may or may not be a dedicated line for pre-registration badge pickup, depending on when you arrive, how long the line is, available staff, etc.

Cash Purchase

Badges will be available for purchase on-site at DEF CON. All badge sales are **cash only**. No checks, money orders, credit cards, etc., will be accepted. In order to keep the registration line moving as quickly as possible, please have **exact change** ready as you near the front of the line.

There are no refunds given for cash sales. If you have any doubt about your desire to buy a badge, please refrain from doing so.

We are unable to provide printed receipts at the time of the sale. A generic receipt for the cash sale of a badge will be made available on media.defcon.org after the conference. You are welcome to print your own copy of the receipt on plain paper.

Via BlackHat

If you've purchased a DEF CON badge as part of your Black Hat registration, you're in luck - you will be able to pick up your DEF CON badge at Black Hat on Thursday. Please bring your Black Hat badge and watch for emails from Black Hat about where exactly the badge pickup will be.

Please note that DEF CON is not able to access or verify Black Hat registration or attendee info. DEF CON's preregistration list is not the same as Black Hat's. For help, ask at Black Hat registration or the concierge area.

Misc

Want to buy multiple badges? No problem! We're happy to sell you however many badges you want to pay for.

If you lose your badge, there is unfortunately no way for us to replace it. You'll have to buy a replacement at full price. Please don't lose your badge. :(

If you are being accompanied by a full-time caretaker (such as someone who will push your wheelchair, and will accompany you at all times), please ask to speak to a Registration Goon. Your caretaker will receive a paper badge that will permit them to accompany you everywhere you go.

Still need help?

If you have questions about anything regarding human registration that are not addressed here, please ask to speak to a Registration Goon.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Hunting for Cryptographic Ghosts: A Bug Hunter's Guide to Signature Malleability and Replay Attacks in EVM Bridges & Multi-Sigs

Tags: Bug Bounty Village | Creator Talk/Panel

When: Friday, Aug 7, 15:30 - 15:59 PDT

Where: LVCCW Level 1 Hall 3 1102 (Creator Stage 6) - [Map](#)

Description:

In the realm of Web3 bug bounties, smart contract logical flaws are highly sought after, but the most devastating, seven-figure bounties often lie within fundamental cryptographic implementation errors. Specifically, ECDSA signature malleability and faulty multi-signature threshold state management are responsible for the biggest bridge drains in history. Yet, many traditional bug bounty hunters steer clear due to the perceived mathematical complexity. This presentation demystifies these high-value bug classes. We will break down exactly how the EVM processes cryptographic signatures (ecrecover), how the mathematical symmetry of elliptic curves allows a single valid signature to be altered into a second, legally distinct signature, and how this can be weaponized to bypass multi-signature validation logic. Attendees will walk away with an actionable, repeatable hunting methodology, custom scripts to automate signature vulnerability testing, and real-world case studies of massive payouts achieved without looking at single line of standard frontend code.

Speakers: Samet Berk Simsek, Ahmet Furkan Aydogan

SpeakerBio: Samet Berk Simsek

Samet Berk Şimşek is a Turknet Cyber Security Specialist & Web3 Developer

SpeakerBio: Ahmet Furkan Aydogan

Ahmet Furkan Aydogan is a Tenure-Track Assistant Professor in the Computer Science Department at the University of North Carolina Wilmington (UNCW). He earned his Ph.D. in Digital and Cyber Forensics Science from Sam Houston State University (SHSU) in 2024, with a focus on Cyber Security, Cryptology, Machine Learning, IoT, and Human-Computer Interaction. His research includes a Brain Frequency-Based Evolutionary Encryption Method for IoT Devices. Ahmet has received multiple awards and has published widely in the fields of cybersecurity and digital forensics.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Hunting the Contagious Trader Delivery Network

Tags: Recon Village | Creator Workshop

When: Saturday, Aug 8, 10:00 - 12:30 PDT

Where: LVCCW Level 1 Hall 2 501 (Recon Village) - [Map](#)

Description:

North Korean threat actors are running one of the largest software supply chain campaigns ever observed in the npm ecosystem, and the infrastructure hiding it in plain sight is discoverable through open-source reconnaissance alone.

This workshop walks participants through how we mapped a live DPRK delivery network targeting cryptocurrency developers, starting from a single malicious npm package and expanding outward to uncover 50+ malicious packages, 100+ GitHub repositories, 30+ throwaway npm personas, 20+ rotating C2 domains, and a social media promotion layer spanning X and Reddit.

The investigation surfaces three malware families: PromptMink, ClipViper, and OtterCookie, which operate through what initially appeared to be separate campaigns but share overlapping infrastructure, actors, and delivery techniques.

The workshop focuses on the recon methodology behind the mapping through six hands-on modules:

- Dependency chain tracing: How malicious payloads hide one to three hops deep in transitive npm dependencies, evading surface-level code review and automated scanners
- Actor network pivoting: Using email patterns, SSH key reuse, shared C2 infrastructure, and build artifact fingerprints to link 30+ throwaway npm accounts into operational clusters
- Identity spoofing detection: How to catch developer identity theft through timezone offset analysis
- GitHub delivery front reconnaissance: Tracing 40+ fork chains across front organizations all serving identical malicious payloads behind bot-inflated star counts and SEO-stuffed descriptions
- Social media promotion mapping: Connecting verified X accounts and Reddit personas to the distribution layer, and observing how the social infrastructure persists even after GitHub takedowns
- Evasion tracking in real time: Documenting the operators' shift from obfuscated JavaScript to on-chain payload storage via Solana, where the npm package contains zero malicious code and the payload lives in a blockchain account beyond the reach of static analysis

Participants work directly with actionable IoCs (packages, C2 domains, SSH keys, YARA rules, detection queries) and leave with a breakdown of how current Contagious Interview and Contagious Trader toolsets are converging into a unified threat.

Attendees will leave with a repeatable framework for mapping supply chain malware delivery networks using open-source data: package registries, Git metadata, DNS records, social media artifacts, and cross-referencing with community threat feeds.

Speakers: Alessandra Rizzo, Ariel Ropek

SpeakerBio: Alessandra Rizzo

No BIO available

SpeakerBio: Ariel Ropek

No BIO available



Radio Frequency Village - Saturday - 16:30-17:25 PDT

Title: I'm Not Special, and You Can Too! A journey into RF Antenna Design for Dummies.

Tags: Radio Frequency Village | Creator Talk/Panel

When: Saturday, Aug 8, 16:30 - 17:25 PDT

Where: LVCCW Level 1 Hall 1 409 (Radio Frequency Village) - [Map](#)

Description:

Take a walk with Hamspiced from Midwest Gadgets as he explains, with an appropriate amount of sarcasm and emotional damage, how to make an LC tank circuit from scratch.

This talk will cover the basic theory behind inductance, capacitance, resonance, and why math has a terrible habit of being correct even when your prototype is not. From there, we will move into design, simulation, PCB layout, testing, tuning, and the deeply humbling process of discovering that “close enough” is absolutely not close enough at 13.56 MHz.

Using open-source tools and real-world examples from Midwest Gadgets hardware, this talk follows the full maker journey: theory, design, prototyping, failure, more failure, brief hope, additional failure, and eventually something that works well enough to accidentally become a product.

Attendees do not need to be RF engineers, electrical engineers, or people who enjoy reading datasheets for fun. This talk is meant for makers, hackers, badge builders, hardware weirdos, and anyone who has ever stared at a PCB and thought, “This should work,” immediately before it did not.

By the end, you will understand the basic concepts behind LC tank circuits, how to approach designing one, what tools can help, what mistakes to expect, and why failure is less of a roadblock and more of a mandatory subscription service. Most importantly, you will see how open-source tools, persistence, and a questionable amount of stubbornness can turn a pile of bad revisions into working hardware."

SpeakerBio: Hamspiced, Owner, Midwest Gadgets

Hamspiced (Nick Gambino) is a maker, technologist, and founder of Midwest Gadgets LLC, where he designs hardware tools for hackers, makers, and security researchers. His work focuses on RF exploration, NFC systems, embedded development, wardriving, and open-source hardware.

With a background in event and exposition technology leadership, Hamspiced combines hands-on engineering with practical product design and community-focused education. His work is driven by curiosity, accessibility, and the belief that understanding technology gives people greater agency.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

The Diana Initiative - Friday - 11:50-11:59 PDT

Title: ICS Village Tour

Tags: The Diana Initiative | Creator Tour

When: Friday, Aug 7, 11:50 - 11:59 PDT

Where: LVCCW Level 1 South Lobby / Atrium - [Map](#)

Description:

Interested in visiting ICS Village but afraid to go by yourself? The Diana Initiative is hosting tours! Follow a volunteer to ICS Village and be introduced to the community and activities inside!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: ICSForge: (Open-Source) OT/ICS Security Coverage Validation Platform

Tags: ICS Village | Creator Talk/Panel

When: Friday, Aug 7, 14:30 - 14:59 PDT

Where: LVCCW Level 1 Hall 3 801 (Creator Stage 1) - [Map](#)

Description:

ICSForge is an open-source OT/ICS Security Coverage Validation Platform designed to help defenders, SOC teams, and OT security engineers validate detection, visibility, and readiness against real-world industrial attack techniques.

ICSForge is built to tackle a critical gap in OT/ICS security. It aims to solve a real problem “How do I safely validate OT security countermeasures from functionality, visibility and detection coverage perspective by using industrial traffic and MITRE ATT&CK® Matrix for ICS?” The goal is simple; make it easier to answer “Are we actually seeing, detecting, controlling and protecting what we think we are?”

OT defenders have no practical and safe way to validate whether their network security monitoring sensors, firewalls, and segmentation controls actually detect and/or protect against real ICS attack techniques. By focusing on security coverage validation in industrial environments, the goal is to move beyond assumptions and provide measurable assurance for detection capabilities in critical infrastructure.

ICSForge focuses on what can actually be observed on the network and generates realistic OT traffic and PCAPs (500+ scenarios) in 10 industrial protocols (Modbus/TCP, DNP3, S7comm, IEC-104, OPC UA, EtherNet/IP, BACnet/IP, MQTT, GOOSE, PROFINET DCP) which are aligned with 68 out of 83 unique techniques in MITRE ATT&CK for ICS v18 (82% coverage) -without exploiting real systems or causing unsafe process impact- to help asset owners and defenders assessing the quality of existing security countermeasures such as firewalls, OT NSM sensors and ACLs and identifying hidden gaps.

Most OT/ICS security tools promise coverage, very few let you prove it. ICSForge helps you answer questions like: - Can my Network Security Monitoring/IDS actually see Modbus manipulation attempts? - Which MITRE ATT&CK for ICS techniques are observable on the wire? - Do my detections fire when realistic OT traffic is sent? - Do my IT/OT firewalls or ACLs work as expected and blocks potentially harmful traffic? - What do I miss today, and why?

ICSForge is developed with a safe-by-design approach, operating within a Sender-Receiver architecture and interacting only with the designated sender and receiver, without touching other OT devices.

SpeakerBio: Can Kurnaz

Can (pronounced as /d%¾ n/ or John) works as an Industrial Control Systems (ICS) / Operational Technology (OT) Cybersecurity Specialist and has over a decade of professional experience in cybersecurity field, focused on OT/ICS Cyber Defense such as secure architecture development, OT/ICS monitoring, endpoint security platforms and vulnerability management. He has offensive security background such as penetration testing, red teaming, OT/ICS site security assessments and also has experience in incident response and cybersecurity trainings (both hands-on and awareness). His passion is protecting the critical infrastructure and production environments by providing technical knowledge on multiple cybersecurity domains which help for preparation, prevention, detection and response. Can has presented several times at leading cybersecurity conferences such as Black Hat, DEF CON and SANS Summits and he holds GRID, GICSP, OSCP, OSWP, ISA/IEC 62443 Expert (CFS, CRAS, CDS, CMS) certifications.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Identity Crisis: Novel Vulnerabilities leading to Kerberos Downgrade, DoS, and Full Domain Takeover

Tags: DEF CON Official Talk | Demo | Tool | Exploit

When: Saturday, Aug 8, 10:00 - 10:59 PDT

Where: LVCCW Level 1 Hall 3 906 (Main Track 3) - [Map](#)

Description:

Active Directory remains a major component of modern enterprise networks, and its security is paramount. Active Directory attack campaigns often aim to achieve Domain Admin privileges, which allow complete control over the domain. But what if we could simply confuse domain controllers, causing them to identify us as someone else? In this talk, we'll dive into Kerberos and Active Directory and show how curiosity and creative thinking led to the discovery of two new identity confusion vulnerabilities. The first vulnerability, KerberLoss (CVE-2026-25177), bypasses a forest-wide security mechanism to perform a Denial of Service, or even force authentication to downgrade from Kerberos to NTLM. We later discovered ResetNightmare (CVE-2026-27912): a logical flaw in a Kerberos mechanism, allowing low-privileged users to compromise any account in the domain, including domain admins, leading to full domain takeover. The vulnerability is surprisingly easy to exploit and has a single, common prerequisite, making it highly dangerous for unpatched environments. We'll explain the vulnerabilities, show them in action, and share practical detection opportunities and mitigation strategies to reduce exposure. In addition, we'll be releasing a tool that automatically runs the entire attack flow for simple experimentation and testing.

SpeakerBio: Shai Laron, Semperis

Shai Laron is a Security Researcher with 6 years of experience, focusing on Active Directory, Windows, and Identity Security, working at Semperis' Research team. He has a strong passion for researching Kerberos and has discovered multiple vulnerabilities related to it.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: IDEViewer - Securing Developer Workstations from IDE Supply Chain Threats

Tags: Intermediate | AppSec Village | Creator Event/Activity

When: Friday, Aug 7, 15:15 - 16:15 PDT

Where: LVCCW Level 1 Hall 2 604 (Appsec Village) Arsenal - [Map](#)

Description:

IDEViewer is an open-source, cross-platform security tool that continuously monitors developer workstations for supply chain threats originating from IDE extensions, software dependencies, plaintext secrets, and AI development tools.

Developer IDEs have become a high-value attack surface. Malicious or over-permissioned VS Code extensions can execute arbitrary code, exfiltrate secrets, and establish persistence. npm lifecycle hooks in dependencies run silently during install. AI coding assistants like Claude Code, Cursor, and MCP servers introduce new data exfiltration vectors through unchecked permissions and network access. IDEViewer addresses this blind spot by scanning extensions across 7+ IDEs, analyzing their permissions against a risk model, detecting plaintext secrets, inventorying all installed packages (including those bundled inside extensions), monitoring for git hook bypasses, and detecting AI tool configurations with their associated permissions.

SpeakerBio: securient

Vinod is a Staff Security Engineer at PIP Labs and IEEE Senior Member with over a decade of cybersecurity experience spanning financial services, government, and tech. His career across Amazon, Zapier, and HackerOne has built deep expertise in penetration testing, cloud security architecture, and application security across AWS, GCP, and Azure — now applied at the intersection of traditional enterprise security and Web3/blockchain infrastructure. He is an author and reviewer for the HTTP Archive's Web Almanac, organizer of the Blockchain Security Village at Seaside, and creator of the open-source API Doc Converter Burp Extension. He actively contributes to the security community through writing on Medium, bug bounty programs, and mentoring aspiring security professionals.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: If I Were Eighteen Again: Career Advice for the AI Era

Tags: Noob Community | Creator Talk/Panel

When: Friday, Aug 7, 11:45 - 12:45 PDT

Where: LVCCW Level 1 Hall 4 1417 (Noob Community) - [Map](#)

Description:

Please Note: This talk is based on the post "If I were Eighteen Again", published June 16, 2025 from my personal blog (<https://securing.dev/posts/if-i-were-eighteen-again/>).

Abstract

In 2025 the CEO of Anthropic stated that AI could eliminate half of all entry-level white collar jobs within five years. For n00bs entering the cybersecurity industry today, that's a scary headline; It doesn't have to be a death sentence for your nascent career.

In this talk the speaker shares what they would do differently if they were eighteen again, drawing from their own experiences entering the workforce at the bottom of the 2008 housing market crash with no connections, no work history, and no roadmap. Reflecting on over a decade of acquiring and building skills as an Information Security practitioner, this session delivers timeless, practical advice that will help aspiring security professionals build a career that is resilient to economic downturns, immune to hype cycles, and capable of surviving whatever the latest technology trend comes next.

Detailed Outline

Introduction (4 minutes)

- \$WHOAMI
- The AI jobs headline, and why it's both alarming and useful
- What this talk is, and what it isn't: timeless career advice, not a silver bullet
- Some caveats: lived experience, privilege, and why your mileage may vary

Read & Write Long-Form Content (6 minutes)

- The world's most successful people are avid readers
- Reading vs. watching/listening: what the neuroscience actually says
- Algorithmic recommendation engines and the danger of passive consumption
- Writing as a skill multiplier: building a body of work before you need it
- "Do it scared", and overcoming the fear of publishing
- When to update your public opinions, and why doing so is a superpower

Learn How to Learn (6 minutes)

- The difference between *knowing* something and *being able to do it*
- Identifying your own learning style before committing to expensive programs
- The "Read, Do, Write, Relax" loop for accelerating and sustaining skill development
- How to take effective breaks without losing momentum
- Avoiding the regret of wasted time in your youth

Develop Critical Thinking & Practice Mindfulness (6 minutes)

- Charlie Munger's rule: never hold an opinion without knowing the other side's argument(s) better than they do
- Building a mental network of ideas that current LLMs have difficulty replicating
- Mindfulness as a career superpower, from financial decisions to skill development
- Practical intro to meditation: apps, tools, and building a consistent practice
- Presence of mind as the thing that separates good practitioners from great ones

Build & Maintain a Public Brand (7 minutes)

- The NPC vs. PC analogy: passive individuals are losing the career game
- Why employers now expect a body of work before they'll consider you
- Real-world example: how a recent college grad landed a Senior role right out of school
 - ◆ Olivia Gallucci
- Platforms, formats, and how to start from zero
- Why public content is the new resume

Seek Out Mentorship (6 minutes)

- Why mentors won't look for you — and how to make yourself worth mentoring
- The mistake of asking for things without putting in the work first
- Building a portfolio of mentors across different career dimensions (IC, leadership, business)
- How to approach potential mentors without being annoying about it
- My own mentor network, and what I've learned from each of them

Thoughts on Formal Education, Certs & Bootcamps (6 minutes)

- Is a four-year degree still worth it? (Honest answer: it depends)
- The community college + top school financial aid strategy
- CTF > CCDC for real-world skill development and job opportunities
- Which certifications actually matter: practical exams vs. paper tests
- Why bootcamps are basically a money trap in the LLM era
- The three things leaders look for in junior talent: Attitude, Aptitude, and Engagement

On AI and Skill Development (6 minutes)

- Using LLMs well vs. using them as a crutch
- Why having AI write your public content is both cheap and easy to spot
- The whiteboard technique for working with LLM-generated-anything
- How LLMs narrow your thinking, and how to fight back against that

The AI-Averse Path: Becoming a Shokunin (5 minutes)

- What the Japanese concept of *shokunin* has to do with your career
- Craftsmanship as a defense against commoditization
- What this path actually requires, and why it's harder than it sounds

Q&A (8 minutes)

Attendee Takeaways

Foundational habits that compound: Reading, writing, mindfulness, and continuous learning are not just “soft skills”, they are what separates practitioners who plateau from those who build enduring careers.

Your public brand is your resume: In 2026, a body of published work is the difference between being considered for a role and being filtered out.

AI is a tool, not a replacement for thinking: Understanding how to use LLMs without outsourcing learning or critical thinking is one of the most important skills a new practitioner should be developing right now.

Education and certifications are tools, not guarantees: Know what they are actually buying you, and pursue practical proof of skill development over paper credentials wherever possible.

SpeakerBio: Keith Hoodlet

No BIO available

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

The Diana Initiative - Saturday - 14:00-14:10 PDT

Title: Illumicon Tour

Tags: The Diana Initiative | Creator Tour

When: Saturday, Aug 8, 14:00 - 14:10 PDT

Where: LVCCW Level 1 South Lobby / Atrium - [Map](#)

Description:

Interested in visiting Illumicon but afraid to go by yourself? The Diana Initiative is hosting tours! Follow a volunteer to Illumicon and be introduced to the community and activities inside!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Social Gatherings/Events - Saturday - 21:00-00:59 PDT

Title: Illuminati Party

Tags: Party

When: Saturday, Aug 8, 21:00 - 00:59 PDT

Where: LVCCW Level 3 W327 (Misc Meeting Room) - [Map](#)

Description:

It's time to get under the hood and rewrite the rules of engagement. If we want a future where explorers aren't outlaws, we have to start by taking over the room—so join us for the Illuminati Party, where our crew gathers to set the parameters for the night. Come share your passion, plot the future, and help us amplify the community.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Imposter Syndrome Is Distracting You From the Work That Matters

Tags: Noob Community | Creator Talk/Panel

When: Saturday, Aug 8, 16:15 - 16:45 PDT

Where: LVCCW Level 1 Hall 4 1417 (Noob Community) - [Map](#)

Description:

Cybersecurity has an imposter syndrome problem, and it isn't just personal — it's structural. The field is so wide that no single human can cover it, which means even five-year practitioners feel behind. New entrants interpret that feeling as evidence they don't belong, and the field loses exactly the people it needs most: the pattern-recognizers, the communicators, the artists, the networkers, the non-stereotypical thinkers. This 30-minute talk reframes imposter syndrome as a misread of a real signal. It makes the case that cybersecurity is the defining fight of this era — and argues that now, when AI is shifting the terrain and some people are throwing in the towel thinking they're already behind, is exactly when we need warriors who understand that every generation has faced unfamiliar ground. We shouldn't deny ourselves a tradition of fighting simply because the landscape has changed. The next generation of warriors won't look like the picture in your head — and they need to be you. The talk moves through three acts. First, it names the lie of "being behind" — the field is too big for any one human, and feeling inadequate is evidence you're perceiving its size correctly, not a verdict on you. Second, it makes the stakes concrete: hospitals diverting ambulances during ransomware events, ICAC task forces doing digital forensics on devices seized from predators, dissidents whose phones are compromised by state actors. The technical failure and the human failure are the same event seen from opposite ends of the same wire. Third, it widens the door: DFIR, GRC, threat intelligence, security awareness, policy, AppSec partnership — the field has roles for thinkers who don't fit the hoodie-in-a-basement stereotype, and it needs them urgently. If you're sitting in N00b Village wondering whether you belong here, this talk is for you. The voice telling you everyone else belongs more is wrong about you, and it's wrong about the field. Stay.

SpeakerBio: Samantha Schwartz

No BIO available

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Social Engineering Community Village - Friday - 12:00-12:59 PDT

Title: Improv

Tags: Social Engineering Community Village | Creator Event/Activity

When: Friday, Aug 7, 12:00 - 12:59 PDT

Where: LVCCW Level 3 W317-319 (Social Engineering Community Village) - [Map](#)

Description:

Join Bryan and Kevin for a fun, low-pressure improv showdown where quick reactions, creative thinking, and social engineering skills take center stage.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Blacks In Cyber Village - Saturday - 16:00-16:30 PDT

Title: Improving Security Vulnerability Descriptions using LLMs

Tags: Blacks In Cyber Village | Creator Talk/Panel

When: Saturday, Aug 8, 16:00 - 16:30 PDT

Where: LVCCW Level 3 W322-W324 (BIC Village) - [Map](#)

Description:

CVE records are a foundation of modern vulnerability management, but many entries still contain incomplete, vague, or low-context descriptions. This limits their usefulness for security teams, researchers, and automated tools that rely on CVE text to understand and communicate risk. This talk presents research on using large language models to enrich CVE descriptions with additional vulnerability context. By combining information from CWE, CVSS, and proof-of-concept code, the approach generates clearer and more informative vulnerability descriptions. The enriched descriptions are then evaluated through MITRE ATT&CK technique classification to measure whether they improve downstream security analysis. Results show that structured prompting can make vulnerability descriptions more interpretable and improve classification performance, achieving up to a 12.7% F1 score increase over original CVE text. This work highlights how LLMs can support vulnerability analysis, strengthen security communication, and help transform incomplete vulnerability records into more actionable cyber threat intelligence.

SpeakerBio: Kenechukwu Nwodo, Ph.D. Student, Virginia Tech / Co-founder, WayWave Inc.

Kenechukwu Nwodo is a Ph.D. student in the Bradley Department of Electrical and Computer Engineering at Virginia Tech, where their research interests include software and mobile security. Originally from Lagos, Nigeria, Kene is also the co-founder of WayWave Inc., where they lead the development of advanced localization solutions.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: In Untrust We Can Trust: Enforcing Trust Boundaries for Humans and AI Alike

Tags: Intermediate | AppSec Village | Creator Event/Activity

When: Saturday, Aug 8, 10:15 - 11:15 PDT

Where: LVCCW Level 1 Hall 2 604 (Appsec Village) Arsenal - [Map](#)

Description:

We keep saying “never trust user input.” Yet our frameworks still do not differentiate between trusted data and attacker-controlled data.

OWASP Untrust is an OWASP umbrella project built around a simple invariant: all data is implicitly untrusted and may cross security boundaries only through deliberate, verifiable trust transitions.

Through projects like VV (Validated Values) and BoxedPath, implemented across Python, Java, C#, C++, and Node.js, Untrust makes unsafe states structurally difficult to represent.

Instead of detecting vulnerabilities after they are written, Untrust enforces trust boundaries by construction for humans and AI alike.

SpeakerBio: Yariv Tal

Yariv Tal is a senior developer, security researcher, and cofounder of Secure From Scratch, a venture dedicated to teaching developers secure coding from the very first line of code.

A summa cum laude graduate of the Technion, Yariv brings four decades of programming experience and years of university lecturing and bootcamp mentoring to the field of application security.

He lectures on secure coding in academia and the private sector, leads the OWASP-untrust project, and researches the intersection of AI and application security, with a focus on secure code generation, LLM evaluation, and secure-by-construction development.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Incident Response 101: Preparing Before the Hack, Responding After It

Tags: Blue Team Village | Creator Talk/Panel

When: Friday, Aug 7, 10:00 - 10:59 PDT

Where: LVCCW Level 2 W217 (Blue Team Village) Main Stage - [Map](#)

Description:

When an organization gets hacked, recovery is only part of the challenge. Security teams must quickly determine what happened, contain the threat, remove the attacker, and restore operations without allowing the incident to happen again. That work falls to incident responders, the cybersecurity professionals who investigate attacks, coordinate response efforts, and help organizations recover under pressure.

This beginner-friendly session introduces the role of the incident responder and explains how incident response works across the major stages of preparation, detection, containment, eradication, recovery, and post-incident improvement. Attendees will leave with a practical understanding of what incident responders do, why their work matters, and how structured response processes help organizations reduce damage and improve resilience after a cyber incident.

SpeakerBio: Joshua Morgan

Joshua Morgan is a seasoned information security expert and passionate educator, dedicated to empowering the next generation of security professionals. With a strong background in the Blue Team realm, Joshua brings hands-on experience and real-world expertise to his work as an instructor at a local university, teaching advanced information security concepts to Masters-level students.

As a respected speaker in the industry, Joshua has had the opportunity to share his knowledge with a wider audience, having presented at leading conferences such as DEF CON and BSides. His involvement in the security community extends beyond the stage, as he collaborates with fellow security enthusiasts and mentors newcomers to the industry.

Joshua's commitment to security education and community outreach has made him a valuable asset to the industry, and his passion for securing all aspects of life continues to drive his work.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Blue Team Village - Saturday - 17:00-17:59 PDT

Title: Incident Response in 2026

Tags: Blue Team Village | Creator Talk/Panel

When: Saturday, Aug 8, 17:00 - 17:59 PDT

Where: LVCCW Level 2 W217 (Blue Team Village) Main Stage - [Map](#)

Description:

Join us at the Blue Team Village for an interactive session on the shifting dynamics of Incident Response. As modern threat vectors evolve, security teams must actively adapt their core competencies and refine their playbooks. Our panel of practitioners will dive into practical strategies for navigating high-pressure environments—balancing technical depth with stakeholder management, and building resilience against burnout. We will discuss critical operational mistakes, the role of automation, and how to foster a collaborative IR community. Whether you are a seasoned responder or just starting your journey, gain actionable insights on advancing your IR career while maintaining your sanity.

Speakers: Chriss Hansen, K Singh, Levone Campbell, Sarthak Taneja

SpeakerBio: Chriss Hansen

Chriss Hansen is a seasoned Cyber Field Engineer at Pentera, with a background as a Digital Forensic Engineer and extensive experience in DFIR roles for various companies. He serves as an Incident Response Lead for the Wisconsin Cyber Response Team, leveraging his expertise to combat cyber threats. Prior to his cybersecurity career, he worked as a mattress salesman at Mattress Firm. Outside of work, he enjoys water polo, running, riding motorcycles, and playing the drums, showcasing his diverse interests beyond the tech world. He is also on the board for DC608: a non-profit educational group in Madison Wisconsin based on training and educating future cyber security experts.

SpeakerBio: K Singh

"K" Singh is a Senior Incident Response Consultant at Mandiant, where he helps Fortune 500 companies, leading enterprises, and a wide range of organizations navigate high-stakes cybersecurity incidents. With experience spanning large-scale incident response, tabletop exercises, strategic security planning, and hands-on “dead disk” forensics, K has seen just about everything under the sun—and then some.

Before joining Mandiant, K served as a Senior Incident Response Consultant at CrowdStrike and as an Incident Response Consultant and Forensic Lab Manager with the Global Incident Response Practice at Cylance.

When he's not untangling cyber crises, K is usually elbows-deep in a car project—grumbling about questionable engineering decisions and breaking things that, by all logic, should never break.

SpeakerBio: Levone Campbell, Chief Information Security Officer

Levone Campbell, MBA, MPS, CISSP

With more than two decades of experience in cybersecurity operations, Levone Campbell serves as a Cybersecurity Lead and Incident Coordinator, helping safeguard his organization's digital environment through strategic defense and incident response.

A seasoned information technology professional, Levone has developed deep expertise in cyber threat intelligence and cybercrime analysis, consistently anticipating and responding to emerging threats in an increasingly complex digital landscape. He has also expanded his focus to include the growing intersection of artificial intelligence and cybersecurity, with particular attention to the evolving challenges of AI-driven threats and defensive capabilities.

Levone's academic background includes dual bachelor's degrees in Management and Marketing from North Carolina A&T State University, a Master of Business Administration from Walden University, and a Master of Professional Studies in Technology Management with a concentration in Cybersecurity from Georgetown University.

His commitment to professional excellence is further demonstrated by his industry-recognized certifications, including the CISSP, which underscore his standing as a well-rounded cybersecurity leader.

Based in Houston, Texas, Levone values the balance between a demanding career and a strong family life. Married for 20 years and a proud father of two, he brings discipline, perspective, and purpose to his work in protecting critical digital assets and advancing cyber resilience.

SpeakerBio: Sarthak Taneja

Started from Offensive Security and ended up in Defense. Wearing Purple hat most of the days.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Telecom Village - Saturday - 15:45-16:45 PDT

Title: Industry Challenges & SOC Reality

Tags: Telecom Village | Creator Talk/Panel

When: Saturday, Aug 8, 15:45 - 16:45 PDT

Where: LVCCW Level 3 W321 (Telecom Village) - [Map](#)

Description:

1. Telecom SOC challenges and operational realities
2. Evolving telecom threat landscape (2G–5G & cloud-native)
3. Telecom-specific attack surfaces and protocol risks
4. Limitations of traditional SOC's in telecom environments
5. Detection challenges across SS7, Diameter, GTP, SIP, and 5G
6. Real-world telecom attacks and fraud scenarios
7. Threat hunting and protocol-aware monitoring
8. AI-driven detection, automation, and response
9. Building a modern Telecom SOC
10. Future security challenges in 5G and beyond

SpeakerBio: Vinod Shrimali

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Inference in the Infrastructure: Developing NIST AI RMF Resources for Resilient AI in Critical Systems -

Tags: Policy @ DEF CON | Creator Talk/Panel

When: Sunday, Aug 9, 12:00 - 12:30 PDT

Where: LVCCW Level 2 W210-211 (Policy Village) - [Map](#)

Description:

As grids decentralize and cyber-attacks accelerate, Critical Infrastructure must keep up. "Inference in the Infrastructure" offers a path to machine-speed defense, but it is only as safe as the guardrails we build together. This is a call to action to help shape the new NIST AI Risk Management Framework Profile for Trustworthy AI in Critical Infrastructure. We need the hacker community to ensure these systems are worthy of our trust before they are fully deployed. Trustworthy AI in critical systems requires more than high-level policy. The hacker mindset is vital for identifying the emergent failures, hidden interdependencies, and non-obvious edge cases. We will dive into resources designed to bridge the gap between governance and field-ready implementation, translating trustworthiness characteristics into actionable "bridge language" and technical practices that facilitate governance controls that align with both data science and operational realities. We are inviting the community to look under the hood, stress-test, and shape the draft guidance before it informs the rules for the next generation of infrastructure. Whether you are an AI researcher, an ICS defender, or a policy architect, your "ground-truth" input is needed to ensure we automate our world on a foundation that is both resilient and intelligent.

Speakers: Raymond Sheh, Martin Stanley

SpeakerBio: Raymond Sheh, Johns Hopkins University

Dr. Raymond Sheh is an AI, cybersecurity, robotics, and standards expert with over two decades of published international research experience across academia, industry, government, and defense. He is an Associate Research Scientist at Johns Hopkins University in Maryland and leads the development of the NIST AI Risk Management Framework (AI RMF) Profile for Trustworthy AI in Critical Infrastructure at the U.S. National Institute of Standards and Technology (NIST) Information Technology Laboratory (ITL). He was previously the Uncrewed Aircraft Systems (UAS) Research Lead for the NIST Public Safety Communications Research Division (PSCR), a Research Professor at Georgetown University in Washington DC, and a Senior Lecturer in Computer Science at Curtin University in Western Australia. Dr. Sheh holds a Ph.D. in AI and robotics from the University of New South Wales in Sydney, Australia.

SpeakerBio: Martin Stanley, U.S. National Institute of Standards and Technology (NIST)

Martin Stanley, AI and Cybersecurity Researcher, leads the NIST AI Risk Management Framework (AI RMF) efforts at the U.S. National Institute of Standards and Technology (NIST), Information Technology Laboratory. Martin previously led the Emerging Technology and R&D Program at CISA and the Enterprise Cybersecurity Program at the U.S. Food and Drug Administration. Prior to his federal service Martin held executive leadership positions at Vonage and UUNET Technologies. Martin co-authored "Digital Health", an Oxford University Press Publication, and led the 2024 development of NIST AI 600-1 "NIST AI RMF: Generative Artificial Intelligence Profile" and NIST SP 800-218A "Secure Software Development Practices for Generative AI and Dual-Use Foundation Models: An SSDF Community Profile."

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

DEF CON Training - Saturday - 08:30-17:30 PDT

Title: Influence Operations: Tactics, Defense, and Exploitation

Tags: DEF CON Training (Paid) (2-day) | DEF CON Training

When: Saturday, Aug 8, 08:30 - 17:30 PDT

Where: LVCCW Level 2 W223 (Training) - [Map](#)

Description:

Speakers:Greg Conti,Tom Cross

SpeakerBio: Greg Conti

No BIO available

SpeakerBio: Tom Cross

No BIO available

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

DEF CON Training - Sunday - 08:30-17:30 PDT

Title: Influence Operations: Tactics, Defense, and Exploitation

Tags: DEF CON Training (Paid) (2-day) | DEF CON Training

When: Sunday, Aug 9, 08:30 - 17:30 PDT

Where: LVCCW Level 2 W223 (Training) - [Map](#)

Description:

Speakers:Greg Conti,Tom Cross

SpeakerBio: Greg Conti

No BIO available

SpeakerBio: Tom Cross

No BIO available

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: InQuorigible: Quora in Missing Persons OSINT

Tags: Recon Village | Creator Talk/Panel

When: Friday, Aug 7, 10:45 - 11:30 PDT

Where: LVCCW Level 1 Hall 3 801 (Creator Stage 2) - [Map](#)

Description:

We all know Quora - or do we? Like Internet herpes, if you're a Google user, it'll follow you, forever, haunting your inbox with clickbait if you Google while logged into your account.

...But do we REALLY know Quora? Because despite being a pustule on the Internet that exists for the sole purpose of spamming SERPs, you'll be shocked to learn that it's also got - spoiler alert!!! - a dark, seedy underbelly. One that I uncovered while volunteering on an MP investigation. One that can yield surprising, disturbing and useful intelligence.

In this talk, I'll explain: 1. The traces Quora leaves behind when something is "limited," "deleted" or a user is "banned." Because on Quora, 'deleted' just nulls the post body while the API keeps serving the slug and author, and 'limited' barely hides anything at all. On Quora, Limited is UNLIMITED, just like Olive Garden's breadsticks! Except unlike Olive Garden breadsticks, Quora's "limited" option is a fig leaf, and "deleted" content isn't much better: The API doesn't hide it. It coughs up the slug and author fully visible to other accounts and even logged-out strangers. 2. How to use Quora's API hairball to see what a user posted and build a network graph 3. What the disturbing subcultures on Quora mean for OSINT 4. Limitations of approach and ideas for automating OSINT

Trigger warnings: This talk may include mention of disturbing topics, though all information will be anonymized / sanitized and no graphic content shared.

SpeakerBio: Miranda Tedholm, Hunting the Golden Fleece in the JSONs of the world. Extremely employable.

Who is Miranda? A reformed academic, a freelance writer sidelined thanks to a tech that can be described as "autocomplete on steroids," and a recent computer science grad, Miranda has been online since the CompuServe days. Yet she was [redacted] years old before she realized that "being really good at finding people online" was a whole subculture, career, and acronym. Despite never having played Pokemon, she collects degrees and credentials like she's gotta catch 'em all. Two bachelor's degrees, a master's, most of a PhD, and probably able to do the Heimlich maneuver (no promises though). But she yearns only for a job.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Inside the Guts of Ransomware

Tags: Crypto & Privacy Village | Creator Talk/Panel

When: Friday, Aug 7, 14:00 - 14:30 PDT

Where: LVCCW Level 1 Hall 3 1104 (Creator Stage 4) - [Map](#)

Description:

Have you ever wondered how malware analysts identify different encryption algorithms in ransomware samples? In this session, I'll explain the design of some algorithms (such as AES, RSA, ChaCha20, etc.) and show you how to identify them using reverse engineering and debugging techniques, and by using ransomware demos from recent incidents.

SpeakerBio: Ashley Hiram Muñoz, Kaspersky - Incident Response Specialist

I currently work as an Incident Response Specialist on Kaspersky's Global Emergency Response Team (GERT). I live in Mexico and have over seven years of experience in Incident Response, Digital Forensics, Malware Analysis, and Reverse Engineering. Before joining DFIR, I worked for two years as a Penetration Tester.

I have collaborated on various Threat Hunting and Threat Intelligence projects.

Additionally, I have been a speaker at international events such as DEFCON (La Villa Hacker), BSides, Ekoparty, 8.8, HackGDL, BugCON, Pwnterrey, and others. I currently teach the Digital Forensics, Malware Analysis, and Incident Response modules in an information security diploma program at UNAM (Universidad Nacional Autónoma de México).

Certifications: GREM, GCFA, GCFR, eCTHP, CHFI.

--

Actualmente me desempeño como Incident Response Specialist en el Global Emergency Response Team (GERT) de Kaspersky, cuento con +6 años de experiencia realizando Respuesta a Incidentes, Análisis Forense Digital, Análisis de Malware y Reversing; previo a dedicarme a DFIR laboré 2 años como Penetration Tester.

He colaborado en distintos proyectos de Threat Hunting y Threat Intelligence.

Adicionalmente, he sido ponente en eventos internacionales como DEFCON (La Villa Hacker), BSides, Ekoparty, 8.8, BugCON, etc.

Actualmente soy profesor de los módulos de Análisis Forense, Análisis de Malware y Respuesta a Incidentes en un diplomado de seguridad de la información de la UNAM.

Certificaciones: GREM, GCFA, eCTHP, CHFI.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Inside the Red Team Cabal: A Decade of Lessons from Enterprise Red Teams

Tags: Red Team Village | Misc

When: Saturday, Aug 8, 10:00 - 10:59 PDT

Where: LVCCW Level 1 Hall 1 309 (Red Team Village) Workshop Stage 1 - [Map](#)

Description:

The Red Team Cabal is an invite-only community of enterprise red team practitioners dedicated to advancing the craft through trusted collaboration, candid discussion, and the sharing of real-world experiences. While organizations, industries, and technologies may differ, red teams consistently encounter many of the same challenges. The Cabal provides a unique forum where practitioners can learn from one another, exchange lessons learned, and collectively mature the practice of adversary emulation.

This panel brings together Red Team Cabal members from diverse internal red teams spanning multiple industries and organizational environments. Collectively, they represent decades of experience building, operating, and evolving enterprise red team programs. Their perspectives offer a rare opportunity to hear how red teaming has changed over the last ten years, what foundational principles have remained constant, and how organizations at different stages of maturity continue to solve remarkably similar problems.

Panelists will discuss the origins and purpose of the Red Team Cabal, the unique role of internal red teams compared to external consulting engagements, and how internal teams create lasting value through adversary emulation, improving detections, identifying and reducing risk, validating security investments, and driving defensive maturity. The discussion will also cover common challenges faced by enterprise red teams, lessons learned from years of collaboration across the community, and practical guidance for building a successful career in red teaming—from breaking into the field to long-term growth and leadership.

Panelists * Jason Strange * Nat Hirsch * David Martinjak * Niru Ragupathy * Wesley Thurner

Speakers: Jason Strange, Wes Thurner

SpeakerBio: Jason Strange

Jason is a former fortune 100 red teamer turned startup security leader. While at work, he's passionate about all things security, software, user/developer experience, and infrastructure. While he's not at work, he's passionate about getting back to work. He also enjoys developing software, blogging, self-hosting, and writing rap songs about his interests and hobbies.

SpeakerBio: Wes Thurner

As a Principal Security Engineer on Intuit's Red Team, Wesley Thurner specializes in offensive security, protecting the global technology platform and its customers from advanced cyber threats. His expertise is built on a distinguished career as an Exploitation Operator within the U.S. Department of Defense's most elite computer network exploitation (CNE) unit. During his service, he led and developed specialized teams for the U.S. Air Force's premier cyberattack squadron and at U.S. Cyber Command (USCYBERCOM).

A recognized thought leader, Wesley co-authored 'Redefining Hacking: A Comprehensive Guide to Red Teaming and Bug Bounty Hunting in an AI-driven World'. He is also deeply involved in the community as a Co-Organizer for the Red Team Village, where he helps bridge the gap between penetration testing and real-world offensive operations.



Title: Install Me Maybe: Turning Claimable VS Code Extension IDs into Supply-Chain Attacks

Tags: DEF CON Official Talk | Exploit

When: Saturday, Aug 8, 16:00 - 16:59 PDT

Where: LVCCW Level 1 Hall 3 906 (Main Track 3) - [Map](#)

Description:

Developer tools trust extension identifiers way more than they should.

A VS Code extension ID like publisher.extension shows up everywhere a dev environment gets set up, and people treat it as the same trusted thing no matter where it's resolved, but it isn't. Extension identity is marketplace-specific. An extension can be trusted and popular in one marketplace while the matching namespace sits unclaimed in another that the main forks actually pull from. Claim that namespace, publish under the same identifier, and a name people already trust now runs your code. It's dependency confusion, but for editor extensions. I've been calling it Extension Confusion.

I'll show where the trust boundary breaks, the IDE quirks that carry these identifiers across the gap, and what happened when I published proof-of-concept extensions to measure it for real.

The scale got out of hand fast: 1M+ callbacks, hundreds of organizations, \$200k+ in bounties, all in under 3 months. Code running on laptops, managed corporate machines, remote dev setups, WSL, and containers, across SaaS, fintech, Fortune 500s, healthcare, government, and universities.

A trusted name, a missing namespace, and the marketplace gap no one was watching.

Editor extensions are supply chain. Treat them that way.

My talk from last year around malicious extensions can be a good intro:

- <https://www.youtube.com/watch?v=wI8ml8WqmQc>

SpeakerBio: Raphael "rcss" Silva

Raphael Silva is a security researcher at Aikido Security, focused on web security, software supply-chain security, and vulnerability research. He has spoken at DEF CON, RootedCON, OWASP Global AppSec, Black Alps and OWASP local chapters, and has also run hands-on activities at DEF CON. His work centers on finding weird trust assumptions in real systems, turning them into clear attack models, and responsibly disclosing the results to vendors and open-source projects.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Installing and Using the Tracelabs VM

Tags: OSINT For Good Community | Creator Talk/Panel

When: Friday, Aug 7, 17:00 - 17:30 PDT

Where: LVCCW Level 1 Hall 4 1307 (OSINT4Good Community) Stage - [Map](#)

Description:

Come learn from the lead developer how to install and use the Trace Labs Virtual Machine, including a live demonstration. Stick around after to get help during a hands-on workshop

SpeakerBio: Jeff "UltraSunshine" G, Trace Labs VM Lead

Jeff is a forensics engineer with a passion for building tools that empower skilled people to do awesome work. That drive shapes their career and their downtime. At work they build tools that investigators rely on to collect, process, and analyze forensic evidence. As a volunteer, they serve as Trace Labs VM Lead, maintaining an OSINT-focused Linux distribution used by people around the world to investigate missing persons cases as part of Search Party CTFs. In their downtime, they foster stray kittens - proof that even the most seasoned toolmaker has a soft spot for a good rescue.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Intercept.js: Runtime-Aware Detection for JavaScript Environments

Tags: DEF CON Demo Labs | Intermediate | Defense/Blue Team | DEF CON Demo Labs

When: Saturday, Aug 8, 14:00 - 14:45 PDT

Where: LVCCW Level 1 Hall 3 1002 (Demo Labs Track 2) - [Map](#)

Description:

Modern attacks increasingly execute inside JavaScript runtimes (browsers, email clients, and embedded app environments) where traditional file-scanning and OS-level controls lack visibility into application-layer behavior. In these contexts, payloads often exist only as in-memory buffers, fetch responses, or dynamically constructed objects. Detection therefore depends not just on inspecting bytes, but on understanding their origin, transformation, and use at runtime.

We present Intercept.js, an open-source detection engine that runs natively within JavaScript environments, combining byte-level inspection with execution context in real time. Built for YARA compatibility, it extends rule evaluation beyond static artifacts by incorporating signals such as origin provenance, user gesture state, MIME inconsistencies, and object construction paths.

This unified model enables detection of threats as they are assembled and executed — including identifying executable buffers built in memory, anomalous data flows, or content whose structure diverges from its declared type.

As a concrete demonstration, we show how HTML smuggling attacks can be intercepted at the moment of payload construction, preventing delivery before artifacts ever reach disk and exposing a class of threats that evade both network and endpoint controls.

SpeakerBio: Rishi Kant

A builder at heart, Rishi has spent his career turning deep technical ideas into real-world impact. He holds a PhD in Electrical Engineering from Stanford, and earned his B.S. in EECS from UC Berkeley. After 4.5 years of advising global high-tech firms at McKinsey & Company, he followed his passion for building and moved into product management. Rishi led product teams at several cybersecurity companies—including Tanium, Authentic8, and Uptycs. Now, as founder of Sekant Security, he's embedding runtime intelligence directly into web browsers to protect users from phishing, ClickFix, unsafe downloads, shadow AI and other emerging online threats.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Intercept.js: Runtime-Aware Detection for JavaScript Environments

Tags: DEF CON Demo Labs | Intermediate | Defense/Blue Team | DEF CON Demo Labs

When: Friday, Aug 7, 15:00 - 15:45 PDT

Where: LVCCW Level 1 Hall 3 1002 (Demo Labs Track 2) - [Map](#)

Description:

Modern attacks increasingly execute inside JavaScript runtimes (browsers, email clients, and embedded app environments) where traditional file-scanning and OS-level controls lack visibility into application-layer behavior. In these contexts, payloads often exist only as in-memory buffers, fetch responses, or dynamically constructed objects. Detection therefore depends not just on inspecting bytes, but on understanding their origin, transformation, and use at runtime.

We present Intercept.js, an open-source detection engine that runs natively within JavaScript environments, combining byte-level inspection with execution context in real time. Built for YARA compatibility, it extends rule evaluation beyond static artifacts by incorporating signals such as origin provenance, user gesture state, MIME inconsistencies, and object construction paths.

This unified model enables detection of threats as they are assembled and executed — including identifying executable buffers built in memory, anomalous data flows, or content whose structure diverges from its declared type.

As a concrete demonstration, we show how HTML smuggling attacks can be intercepted at the moment of payload construction, preventing delivery before artifacts ever reach disk and exposing a class of threats that evade both network and endpoint controls.

SpeakerBio: Rishi Kant

A builder at heart, Rishi has spent his career turning deep technical ideas into real-world impact. He holds a PhD in Electrical Engineering from Stanford, and earned his B.S. in EECS from UC Berkeley. After 4.5 years of advising global high-tech firms at McKinsey & Company, he followed his passion for building and moved into product management. Rishi led product teams at several cybersecurity companies—including Tanium, Authentic8, and Uptycs. Now, as founder of Sekant Security, he's embedding runtime intelligence directly into web browsers to protect users from phishing, ClickFix, unsafe downloads, shadow AI and other emerging online threats.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

ICS Village - Friday - 11:00-11:59 PDT

Title: Intro to Common Industrial Protocol Exploitation

Tags: ICS Village | Creator Talk/Panel

When: Friday, Aug 7, 11:00 - 11:59 PDT

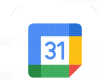
Where: LVCCW Level 1 Hall 3 801 (Creator Stage 1) - [Map](#)

Description:

Intro into Common Industrial Protocol and how to get started finding exploits on CIP enabled devices.

SpeakerBio: Trevor Flynn

Industrial Control Engineer / ICSVillage volunteer / Cyber Security Researcher



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Lockpick Village - Sunday - 13:00-13:30 PDT

Title: Intro to Lockpicking

Tags: Lockpick Village | Creator Event/Activity

When: Sunday, Aug 9, 13:00 - 13:30 PDT

Where: LVCCW Level 1 Hall 1 407 (Lockpick Village) - [Map](#)

Description:

New to lock picking? Haven't picked in a year and need a refresher? Don't know a half-diamond from a turner? This talk is for you! Join one of our knowledgeable village volunteers as we walk you through the very basics of lock picking, from how to hold your tools to the theory behind the technique that makes lock picking possible.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Lockpick Village - Friday - 10:15-10:45 PDT

Title: Intro to Lockpicking

Tags: Lockpick Village | Creator Event/Activity

When: Friday, Aug 7, 10:15 - 10:45 PDT

Where: LVCCW Level 1 Hall 1 407 (Lockpick Village) - [Map](#)

Description:

New to lock picking? Haven't picked in a year and need a refresher? Don't know a half-diamond from a turner? This talk is for you! Join one of our knowledgeable village volunteers as we walk you through the very basics of lock picking, from how to hold your tools to the theory behind the technique that makes lock picking possible.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Lockpick Village - Sunday - 10:15-10:45 PDT

Title: Intro to Lockpicking

Tags: Lockpick Village | Creator Event/Activity

When: Sunday, Aug 9, 10:15 - 10:45 PDT

Where: LVCCW Level 1 Hall 1 407 (Lockpick Village) - [Map](#)

Description:

New to lock picking? Haven't picked in a year and need a refresher? Don't know a half-diamond from a turner? This talk is for you! Join one of our knowledgeable village volunteers as we walk you through the very basics of lock picking, from how to hold your tools to the theory behind the technique that makes lock picking possible.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Lockpick Village - Friday - 16:00-16:30 PDT

Title: Intro to Lockpicking

Tags: Lockpick Village | Creator Event/Activity

When: Friday, Aug 7, 16:00 - 16:30 PDT

Where: LVCCW Level 1 Hall 1 407 (Lockpick Village) - [Map](#)

Description:

New to lock picking? Haven't picked in a year and need a refresher? Don't know a half-diamond from a turner? This talk is for you! Join one of our knowledgeable village volunteers as we walk you through the very basics of lock picking, from how to hold your tools to the theory behind the technique that makes lock picking possible.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Lockpick Village - Friday - 14:30-14:59 PDT

Title: Intro to Lockpicking

Tags: Lockpick Village | Creator Event/Activity

When: Friday, Aug 7, 14:30 - 14:59 PDT

Where: LVCCW Level 1 Hall 1 407 (Lockpick Village) - [Map](#)

Description:

New to lock picking? Haven't picked in a year and need a refresher? Don't know a half-diamond from a turner? This talk is for you! Join one of our knowledgeable village volunteers as we walk you through the very basics of lock picking, from how to hold your tools to the theory behind the technique that makes lock picking possible.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Lockpick Village - Saturday - 10:15-10:45 PDT

Title: Intro to Lockpicking

Tags: Lockpick Village | Creator Event/Activity

When: Saturday, Aug 8, 10:15 - 10:45 PDT

Where: LVCCW Level 1 Hall 1 407 (Lockpick Village) - [Map](#)

Description:

New to lock picking? Haven't picked in a year and need a refresher? Don't know a half-diamond from a turner? This talk is for you! Join one of our knowledgeable village volunteers as we walk you through the very basics of lock picking, from how to hold your tools to the theory behind the technique that makes lock picking possible.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Lockpick Village - Saturday - 15:00-15:30 PDT

Title: Intro to Lockpicking

Tags: Lockpick Village | Creator Event/Activity

When: Saturday, Aug 8, 15:00 - 15:30 PDT

Where: LVCCW Level 1 Hall 1 407 (Lockpick Village) - [Map](#)

Description:

New to lock picking? Haven't picked in a year and need a refresher? Don't know a half-diamond from a turner? This talk is for you! Join one of our knowledgeable village volunteers as we walk you through the very basics of lock picking, from how to hold your tools to the theory behind the technique that makes lock picking possible.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Lockpick Village - Friday - 13:00-13:30 PDT

Title: Intro to Lockpicking

Tags: Lockpick Village | Creator Event/Activity

When: Friday, Aug 7, 13:00 - 13:30 PDT

Where: LVCCW Level 1 Hall 1 407 (Lockpick Village) - [Map](#)

Description:

New to lock picking? Haven't picked in a year and need a refresher? Don't know a half-diamond from a turner? This talk is for you! Join one of our knowledgeable village volunteers as we walk you through the very basics of lock picking, from how to hold your tools to the theory behind the technique that makes lock picking possible.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Intro to Scratch

Tags: DCNextGen | Creator Event/Activity | Youth

When: Saturday, Aug 8, 10:00 - 10:30 PDT

Where: LVCCW Level 3 W316 (DC NextGen) - [Map](#)

Description:

Are you interested in learning to code but don't know where to begin? This class introduces Scratch, a free visual programming language developed by MIT, and is intended for youth ages 8-16. Use real coding concepts and blocks to develop interactive stories, games, and animations. Come learn how to begin coding in a fun and engaging way and join in with millions of your new global peers. You will need a laptop with Chrome or Edge.

SpeakerBio: N3rd H3Rder

No BIO available

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Introduction to AI-Enhanced Threat Modeling Workshop

Tags: Intermediate | AppSec Village | Creator Workshop

When: Sunday, Aug 9, 10:15 - 12:59 PDT

Where: LVCCW Level 1 Hall 2 604 (Appsec Village) Classroom - [Map](#)

Description:

This workshop introduces the practical world of threat modeling, combining hands-on exercises and real-world scenarios. In particular, we will focus on how AI can enhance your threat modeling work plus introduce the basics of securing AI systems.

We will review some of the latest threat intelligence and attack methods projected for 2026/2027, including vulnerabilities in LLMs and Agentic AI. Participants will engage in practical exercises inspired by real industry projects, such as integrating threat modeling into security-by-design and DevOps/MLOps workflows. Key features include threat-informed defense using MITRE frameworks such as ATLAS for real-world analysis, leveraging threat intelligence libraries to deepen threat understanding, and addressing modern challenges.

By the end of this workshop, you will walk away not just with knowledge but also the ability to start practicing threat modeling effectively in your organization.

SpeakerBio: Robert Hurlbut

Robert brings over 30 years of experience in secure coding, software architecture. Robert started and led the threat modeling program at Bank of America, filled in a similar role at Aquia and was a trainer and coach at Toreon. He is passionate about helping teams identify, communicate, and understand threats and mitigations and enhance workload security through threat modeling.

Robert is a Microsoft MVP for Developer Security and an ISC2 Certified Secure Software Lifecycle Professional (CSSLP). He holds a Master of Science in Cyber Security from Southern New Hampshire University and is a Ph.D. candidate in Space Cybersecurity at Capitol Technology University.

Robert is co-author of the Threat Modeling Manifesto (<https://www.threatmodelingmanifesto.org/>), Threat Modeling Capabilities Model (<https://www.threatmodelingmanifesto.org/capabilities>), and co-host of the Application Security Podcast (<https://appsec.buzzsprout.com/>).

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Malware Village - Friday - 12:10-14:10 PDT

Title: Introduction to Reverse Engineering With Ghidra

Tags: Malware Village | Creator Workshop

When: Friday, Aug 7, 12:10 - 14:10 PDT

Where: LVCCW Level 1 Hall 2 600 (Malware Village) Workshops - [Map](#)

Description:

In this workshop, Dr. Wesley McGrew will be presenting a live and unscripted introduction to using Ghidra to reverse engineer real malware samples, targeting people who are new to malware reverse engineering, but have some programming background.

Dr. McGrew will cover the Ghidra user interface, how to load samples, perform initial processing, and how to navigate around a malicious binary. Then, for most of the workshop time, he will provide commentary, advice, heuristics, and approaches for malware analysis as the workshop group takes a look at one or more samples live on the projector.

This workshop is meant to be interactive, driven by attendee questions and interests. Beyond the essentials needed to load malware into Ghidra, the workshop attendees and Dr. McGrew will be collaborating on the direction of the workshop material.

SpeakerBio: Wesley McGrew, Senior Cyber Fellow at MartinFed

Dr. Wesley McGrew directs research, development, reverse engineering, and offensive cyber operations as Senior Cybersecurity Fellow for MartinFederal. He has presented at DEF CON and Black Hat USA on topics of penetration testing, malware analysis, critical infrastructure, and vintage computing, and has taught self-designed courses on reverse engineering and cyber operations at Mississippi State University. Wesley has a Ph.D. in Computer Science from Mississippi State University for his research in vulnerability analysis of SCADA HMI systems. He has entertained audiences at many DEF CON parties as a house music DJ, as well.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Introduction to RFID

Tags: Physical Security Village | Creator Talk/Panel

When: Friday, Aug 7, 12:30 - 12:59 PDT

Where: LVCCW Level 1 Hall 3 1104 (Creator Stage 4) - [Map](#)

Description:

You know the sound of *beep... Click* when using a badge to enter a door to a building, but how does this work and how can you exploit issues with RFID systems?

This talk will explain the basics of what's inside the readers and the badges, and how they communicate wirelessly. You will learn about the common tools available (Proxmark, Flipper, Keysy), how to get one and how to use it.

NEW THIS YEAR: We will cover real case studies of RFID systems being exploited. What were the designers trying to do, and where did they make mistakes?

In addition to the real case studies, we'll talk about techniques to clone badges, and brute force systems to get access you never had in the first place.

Speakers: Ege Feyzioglu, Karen Ng

SpeakerBio: Ege Feyzioglu, Physical Security Village

Ege is a physical security consultant and educator, specialising in access control systems and embedded electronics. She is currently pursuing a degree in Electrical Engineering. Her work focuses on security education, wireless communications, and the intersection of physical security and electronics. She is one of the Village Leads at the Physical Security Village and currently serves as its Secretary-Treasurer.

SpeakerBio: Karen Ng, Physical Security Village

Karen is a risk analyst and physical security penetration tester by day, and a physical security educator and speaker by night. She has a strong interest in security, delivering trainings on physical security vulnerabilities to a wide range of audiences around the world. Karen comes from a background in engineering and has extensive experience in major event logistics. She is one of the Village Leads at the Physical Security Village, and works with the rest of the PSV team to teach how to recognize and fix security exploits to the community. Graphic design is her passion.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Payment Village - Friday - 11:30-11:50 PDT

Title: Introduction to Vulnerable ATM Badge

Tags: Payment Village | Creator Workshop

When: Friday, Aug 7, 11:30 - 11:50 PDT

Where: LVCCW Level 2 W204-205 (Payment Village) - [Map](#)

Description:

The Payment Village set out to design a badge that represents a purposefully vulnerable ATM for educational use. Providing conference attendees with access to a real ATM is impractical due to its size, weight, and limited accessibility. Instead, the badge offers a portable ATM-inspired platform, available to all, that simulates real-world attack surfaces through interactive challenges. We have five prototypes available to try!

To extend its value beyond DEF CON, the badge will be supported by an online platform featuring learning resources, firmware updates, and community support via a website and Discord. We also have a life-size version of the badge as a fully interactive ATM demonstration for attendees to interact with in the village

SpeakerBio: Vincent Sloan, Software Engineer, GoFundMe

20+ years of experience in payments, spanning e-commerce and crowdfunding; currently leads payments engineering at GoFundMe.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Payment Village - Saturday - 11:30-11:50 PDT

Title: Introduction to Vulnerable ATM Badge

Tags: Payment Village | Creator Workshop

When: Saturday, Aug 8, 11:30 - 11:50 PDT

Where: LVCCW Level 2 W204-205 (Payment Village) - [Map](#)

Description:

The Payment Village set out to design a badge that represents a purposefully vulnerable ATM for educational use. Providing conference attendees with access to a real ATM is impractical due to its size, weight, and limited accessibility. Instead, the badge offers a portable ATM-inspired platform, available to all, that simulates real-world attack surfaces through interactive challenges. We have five prototypes available to try!

To extend its value beyond DEF CON, the badge will be supported by an online platform featuring learning resources, firmware updates, and community support via a website and Discord. We also have a life-size version of the badge as a fully interactive ATM demonstration for attendees to interact with in the village

SpeakerBio: Vincent Sloan, Software Engineer, GoFundMe

20+ years of experience in payments, spanning e-commerce and crowdfunding; currently leads payments engineering at GoFundMe.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Noob Community - Friday - 15:30-16:59 PDT

Title: Introduction to Web Exploitation

Tags: Noob Community | Creator Workshop

When: Friday, Aug 7, 15:30 - 16:59 PDT

Where: LVCCW Level 1 Hall 4 1417 (Noob Community) - [Map](#)

Description:

Before you can secure the web, you have to understand how to break it. This 90-minute hands-on session completely bypasses the static slides to give you a practical, interactive introduction to web exploitation. Led by Roman Bohuk, CEO of SkillBit (formerly MetaCTF), you will explore the core technologies that power the web and learn proven, real-world attack methodologies. Whether you are aiming to break into professional web application penetration testing or just looking to sharpen your CTF skills, you'll get dirty with live vulnerabilities, learn how modern web targets are enumerated, and walk away with a solid, actionable foundation in offensive web security.

SpeakerBio: Roman Bohuk

No BIO available

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Game Hacking Village - Friday - 14:00-14:59 PDT

Title: iOS Game Hacking : From Zero to GOD Mode

Tags: Game Hacking Village | Creator Talk/Panel

When: Friday, Aug 7, 14:00 - 14:59 PDT

Where: LVCCW Level 1 Hall 1 211 (Game Hacking Village) - [Map](#)

Description:

SpeakerBio: M41w4r3

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

DEF CON Training - Tuesday - 08:30-17:30 PDT

Title: IoT Exploitation Masterclass: Hardware & RF Hacking

Tags: DEF CON Training (Paid) (2-day) | DEF CON Training

When: Tuesday, Aug 11, 08:30 - 17:30 PDT

Where: LVCCW Level 3 W320 (Social Engineering Community Village Labs) - [Map](#)

Description:

Speakers: Smriti Gaba, Yianna Paris

SpeakerBio: Smriti Gaba

No BIO available

SpeakerBio: Yianna Paris

No BIO available

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

DEF CON Training - Monday - 08:30-17:30 PDT

Title: IoT Exploitation Masterclass: Hardware & RF Hacking

Tags: DEF CON Training (Paid) (2-day) | DEF CON Training

When: Monday, Aug 10, 08:30 - 17:30 PDT

Where: LVCCW Level 3 W320 (Social Engineering Community Village Labs) - [Map](#)

Description:

Speakers: Smriti Gaba, Yianna Paris

SpeakerBio: Smriti Gaba

No BIO available

SpeakerBio: Yianna Paris

No BIO available

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

The Diana Initiative - Friday - 10:10-10:20 PDT

Title: IOT Village Tour

Tags: The Diana Initiative | Creator Tour

When: Friday, Aug 7, 10:10 - 10:20 PDT

Where: LVCCW Level 1 South Lobby / Atrium - [Map](#)

Description:

Interested in visiting IOT Village but afraid to go by yourself? The Diana Initiative is hosting tours! Follow a volunteer to IOT Village and be introduced to the community and activities inside!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Is Your Fridge Running? Then You Better Catch It - State of Security in Refrigeration Systems

Tags: ICS Village | Creator Talk/Panel

When: Sunday, Aug 9, 11:00 - 11:30 PDT

Where: LVCCW Level 1 Hall 3 801 (Creator Stage 1) - [Map](#)

Description:

Much of modern life depends on cooling systems, from keeping food fresh in grocery stores to storing life-saving medicine. At their core, refrigeration controllers manage the entire process, coordinating field controllers directly connected to the refrigeration components like compressors, fans etc. With tens-of-thousands of devices exposed online, used by the largest retail stores around the world, attacking these controllers could cause huge financial loss and disrupt food and medicine supply chains around the globe.

During the last year we looked at refrigeration controllers from leading vendors in the industry, disclosing more than 30 vulnerabilities. We discovered buffer-overflows, authentication bypasses and remote code execution issues. Furthermore, we discovered ways to exfiltrate sensitive information from devices, allowing attackers to leak ownership and location information and pinpoint attack specific targets.

In our talk, we will deep dive into the refrigeration ecosystem. Including hardware firmware extraction and analyzing it, emulating firmware binaries and showcasing the vulnerability chains we uncovered affecting these systems. Lastly, we will present a real-life video demo presenting an attacker hacking a controller covertly, disrupting normal operations and affecting refrigerators' contents.

SpeakerBio: Amir Zaltzman, Claroty Team82

Vulnerability researcher at Claroty Team82

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: IsMyPhonePwned: Analyzing Android/iOS Phones at Scale

Tags: Mobile Hacking Community | Creator Talk/Panel

When: Sunday, Aug 9, 11:30 - 11:59 PDT

Where: LVCCW Level 1 Hall 3 1100 (Creator Stage 7) - [Map](#)

Description:

Mobile devices have become the primary targets for highly sophisticated, targeted spyware and state-sponsored surveillance, yet validating a suspected compromise remains an adversarial challenge across all sectors. Whether in a corporate enterprise, an investigative newsroom, or a human rights organization, tracking mobile malware forces an impossible binary choice: accept the existential risk of data exfiltration, or initiate traditional forensics. For individual users, journalists, and corporate Incident Response (IR) teams alike, standard forensic methods are deeply destructive, and breaks critical software access. Because specialized forensic workstations are complex and cost-prohibitive, high-risk individuals and organizations often remain completely blind to ongoing breaches.

This talk introduces IsMyPhonePwned, an open-source, non-destructive mobile forensic framework designed to democratize device auditing. It allows anyone to scan for Indicators of Compromise (IoCs) and malware infections directly from a standard web browser over a USB connection. By leveraging WebAssembly and a high-performance stack written entirely in Rust, our framework enables client-side extraction, log parsing, and industry-standard Sigma rule evaluation without rooting, zero software installation, and zero device downtime. We will demonstrate how organizations and individual citizens can bypass complex, destructive investigative bottlenecks and perform rapid, privacy-preserving mobile triage at scale.

SpeakerBio: Desnos Anthony, EDF CERT (CERT-EDF)

I spent my last decade at Google in the Android Security Team, to fight against Android malware ! I'm now working at CERT-EDF, to keep the light on ;)

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Payment Village - Friday - 13:30-13:59 PDT

Title: It's a Payment Terminal. It's My Arcade. It's Everywhere. It Cost Me Nine Bucks.

Tags: Payment Village | Creator Talk/Panel

When: Friday, Aug 7, 13:30 - 13:59 PDT

Where: LVCCW Level 1 Hall 3 1104 (Creator Stage 4) - [Map](#)

Description:

20+ million payment terminals. Hardware-signed. Kernel-verified. Processing live transactions in retail, hospitality, and healthcare worldwide. You've probably tapped one this week. We bought one for nine bucks. Sixty seconds later, we had root over WiFi. Three chained vulnerabilities, fully automated, zero interaction. Plaintext credentials, full filesystem, kernel signature enforcement gone. We made it run Snake. Tetris. Whatever you want it to. A PCI-certified arcade. We reported everything to the vendor. They passed. *"Out of support. Not fixing it."* Except retail-purchased units this year ship with the exact firmware they're walking away from. No update mechanism. No OTA. No advisory. The bugs remain exploitable on devices being sold today. PCI-certified doesn't mean patched. Retail-available doesn't mean current. The bugs you can't patch are the ones already on the counter.

SpeakerBio: Chiao-Lin Yu "Steven Meow", Staff Red Team Security Threat Researcher at Trend AI (Trend Micro)

Chiao-Lin Yu (Steven Meow) is a Staff Red Team Security Threat Researcher at Trend AI (Trend Micro) Taiwan. He holds professional certifications including OSCE3, OSCP, CRT0... and LPT. He has previously spoken at DEF CON (USA), CCC (Germany), BSides Tokyo (Japan), HITCON Training (Taiwan), etc. He has disclosed over 50 CVE vulnerabilities affecting major vendors such as VMware, NEC, D-Link, and Zyxel. He specializes in red teaming, web security, IoT, and cats.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Jackpoting? Bypass de EDR? - Hacking ATM

Tags: La Villa Community | Creator Talk/Panel

When: Friday, Aug 7, 16:00 - 16:59 PDT

Where: LVCCW Level 1 Hall 4 1416 (La Villa Community) Main Stage - [Map](#)

Description:

En muchas ocasiones cómo pentesters nos aferramos a la idea de buscar múltiples técnicas de ataque de manera “virtual”, buscando software especializado o creando scripts que nos ayuden a identificar una vulnerabilidad para acceder a un programa o dispositivo en el que nos enfoquemos, pasamos tanto tiempo enfrente de nuestra pantalla, lanzando comandos a lo bastardo hasta ver que podemos encontrar que a veces ignoramos que existen soluciones alternativas y no simplemente de manera virtual, sino de una manera en que podemos tocar, armar y desarmar (esto suele ser menos buscado por pentester, entonces también hay menos documentación).

El proceso de arranque de Windows, conocido como boot process, se divide en varias fases como ya lo vimos: PreBoot (inicialización del firmware BIOS/UEFI y POST), Boot Manager (carga de bootmgr o bootmgfw.efi), OS Loader (ejecución de winload.exe para cargar el kernel) y Kernel Initialization (carga de ntoskrnl.exe y hal.dll, inicialización de controladores y servicios). Finalmente, se inicia winlogon.exe para presentar la interfaz de usuario. Este proceso permite pasar de un estado apagado a un sistema operativo funcional mediante una secuencia jerárquica y verificada.

Respecto a los EDR (Endpoint Detection and Response) basados en el kernel, operan en modo kernel, el nivel más privilegiado del sistema (algunos juegan en UEFI), lo que les permite supervisar actividades de bajo nivel como llamadas al sistema, manipulación de memoria, carga de controladores y acceso a archivos. Al ejecutarse en este modo, los EDR pueden detectar y bloquear amenazas avanzadas como rootkits o malware persistente que intentan eludir las protecciones del modo usuario. Su integración profunda con el kernel les permite realizar monitoreo en tiempo real, análisis de comportamiento y respuesta inmediata ante actividades sospechosas durante y después del arranque.

Normalmente los EDRs se encuentran en KERNEL pero como lo mencione, existen otros que se encuentran en UEFI y si recordamos como funciona windows atrás de UEFI esta SMM entonces es algo un poco más difícil.

Esta charla es pensada para personas interesadas no solo en ATMs y una simple dispensación si no la vista más allá, el análisis y toda la experiencia adquirida cuando te enfrentas a ellos.

Más información sobre el ataque y la teoría detrás de ella:

<https://h0km4.com/posts/DMA-Introduction/>

<https://h0km4.com/posts/telemetry-bypass/>

SpeakerBio: Arnold Jared Morales Yopez, Senior Team Lead, Grupo Salinas

Self-taught in computer security since age 12; holds a degree in Computer Forensics and Cybersecurity and is pursuing a Master's in AI and Cybersecurity.

--

Desde los 12 años, me he dedicado a la informática con un enfoque especial en la seguridad. Actualmente, a mis 22 años, sigo explorando este mundo con la misma pasión, impulsado por la constante evolución de la tecnología y su interminable curva de aprendizaje.

Cuento con una carrera en Cómputo Forense y Ciberseguridad, actualmente curso una maestría en Inteligencia Artificial y Ciberseguridad.

Certificaciones: CWEE | CAPE |CPTS | EWPTX | CRT0 | eMAPT | OSCP | OSCP+ |CEH V13 | EJPT| HTB prolabs Hades - Cybernetics - Zephyr - APTlabs | MDK



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Journey to Create an All-state Cybersecurity Plan for Oklahoma

Tags: Policy @ DEF CON | Creator Talk/Panel

When: Saturday, Aug 8, 10:00 - 10:59 PDT

Where: LVCCW Level 2 W210-211 (Policy Village) - [Map](#)

Description:

This talk will go over the challenges and successes that the State of Oklahoma had in creating an all-of-state cybersecurity plan. It will also offer insights into how we leveraged the State Local Cybersecurity Grants to help shore up defenses in state and local agencies. Finally, I will share personal insights as a grant recipient and what it looks like from the end-user perspective.

SpeakerBio: Craig "jafo" Buchanan, City of Stillwater Oklahoma

Craig Buchanan has worked in government at the city, state, and federal levels. In addition, he worked for over a decade at computer multimedia innovator Creative Labs Inc. He currently works for the city of Stillwater Oklahoma as the security administrator, where his duties include installing and maintaining the city's ever-growing fleet of security cameras, servers, and monitoring devices as well as serving as a professor at Northern Oklahoma College. In his spare time, he volunteers for the American Red Cross doing fraud reviews and serves on the state of Oklahoma's State Local Cybersecurity Grant committee.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

IoT Village - Sunday - 10:00-13:59 PDT

Title: Just Hacking Training

Tags: IoT Village | Creator Workshop

When: Sunday, Aug 9, 10:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 1 215 (IoT Village) - [Map](#)

Description:

2 Mini-Workshops, Only 15 Minutes Each: QEMU: Emulate Your 'Things' – Hack a Drug Lord's Smart Toilet; Encryption! What Encryption? – Decrypt TLS Traffic with mitmproxy. No Schedule.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

IoT Village - Friday - 10:00-17:59 PDT

Title: Just Hacking Training

Tags: IoT Village | Creator Workshop

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 215 (IoT Village) - [Map](#)

Description:

2 Mini-Workshops, Only 15 Minutes Each: QEMU: Emulate Your 'Things' – Hack a Drug Lord's Smart Toilet; Encryption! What Encryption? – Decrypt TLS Traffic with mitmproxy. No Schedule.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

IoT Village - Saturday - 10:00-17:59 PDT

Title: Just Hacking Training

Tags: IoT Village | Creator Workshop

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 215 (IoT Village) - [Map](#)

Description:

2 Mini-Workshops, Only 15 Minutes Each: QEMU: Emulate Your 'Things' – Hack a Drug Lord's Smart Toilet; Encryption! What Encryption? – Decrypt TLS Traffic with mitmproxy. No Schedule.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Blacks In Cyber Village - Friday - 16:00-17:30 PDT

Title: KaliGPT Vibe-Ethical Hacking Session

Tags: Blacks In Cyber Village | Creator Workshop

When: Friday, Aug 7, 16:00 - 17:30 PDT

Where: LVCCW Level 3 W322-W324 (BIC Village) - [Map](#)

Description:

Join B.I.C. Village for KaliGPT Vibe-Ethical Hacking Session, a welcoming session focused on hands-on ethical hacking concepts, Kali Linux workflows, and responsible security learning. Come ready to learn, ask questions, and connect with the community.

SpeakerBio: Timothy E. Bates, Professor of Practice, University of Michigan / Fractional CTO

Timothy E. Bates, also known as "The Godfather of Tech," is a distinguished cybersecurity professional and educator. Discovered as a hacker at age 13 by the U.S. Marshals Service, he was later recruited by the U.S. Government to train on tracking digital pirates and hackers. He brings over 40 years of experience in the tech industry, with extensive expertise in Artificial Intelligence (AI), Blockchain, and Immersive Technologies. His career includes significant roles as Chief Technology Officer (CTO) at Global Fortune 200 companies like Lenovo and General Motors. Timothy currently serves as a Professor of Practice in the College of Innovation & Technology at the University of Michigan-Flint and as a Fractional CTO. He has received numerous accolades, including the BEYA Black Engineers Association Award: Modern-Day Technology Leader.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Social Gatherings/Events - Saturday - 22:00-00:59 PDT

Title: Kayos Klub

Tags: Party

When: Saturday, Aug 8, 22:00 - 00:59 PDT

Where: LVCCW Level 1 North Lobby - [Map](#)

Description:

The Kayos Klub will be a night of music and magic for all ages. To celebrate the life of a lost loved one, we are going all out on a party that will make even the most socially awkward computer nerd want to dance <3.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Keep the Model on Course: Agentic LLM Workflows for Reversing

Tags: La Villa Community | Creator Talk/Panel

When: Saturday, Aug 8, 14:00 - 14:30 PDT

Where: LVCCW Level 1 Hall 4 1416 (La Villa Community) Main Stage - [Map](#)

Description:

Malware analysts are wiring LLMs into their reversing workflows today. The MCP integrations for IDA Pro, Ghidra, radare2, and Binary Ninja are public, and analysts use them to rename functions, triage samples, and hunt vulnerabilities. Adoption has outpaced any measured account of where these tools hold up and where they mislead, and running an agent against one sample can burn an enormous number of tokens on work the model repeats for every binary.

We built an agentic malware analysis framework on ADK (Agent Development Kit) that connects LLMs to disassemblers through MCP, wrapped in per-language skills for C/C++, C#, Go, Android, etc. The ADK agent loop drives the analysis: pulling functions, following xrefs, reading decompiled output, making notes, and issuing disassembler commands on its own. Each skill supplies the runtime context once, so the model spends its budget on the sample. Everything runs in Docker containers for isolation and reproducibility.

We tested it across multiple models on real samples and scored every result against ground truth. Triage and function renaming on stripped binaries work well when the agent is steered. Crypto identification and CVE matching fail in ways that read as authoritative. The analyst is the captain, the model the crew. We ship the containers, skills, and prompt templates so attendees can reproduce similar workflows effortlessly.

Speakers: Asher Davila, Lenin Alevski

SpeakerBio: Asher Davila, Vulnerability Researcher at Palo Alto Networks

Passionate about binary analysis, binary exploitation, reverse engineering, hardware hacking, retro computing, and music.

SpeakerBio: Lenin Alevski, Security Engineer at Google

Lenin Alevski is a Full Stack Engineer and generalist with a lot of passion for Information Security. Currently working as a Security Engineer at Google. Lenin specializes in building and maintaining Distributed Systems, Application Security and Cloud Security in general. Lenin loves to play CTFs, contributing to open-source and writing about security and privacy on his personal blog <https://www.alevsk.com>.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Ham Radio Village - Saturday - 16:00-16:45 PDT

Title: Keeping the Angry Pixies Happy: the Care and Feeding of your Batteries

Tags: Ham Radio Village | Creator Talk/Panel

When: Saturday, Aug 8, 16:00 - 16:45 PDT

Where: LVCCW Level 3 W315 (Ham Radio Village) - [Map](#)

Description:

The talk will cover various battery types. For each type, we will cover such items as why you might want to use it, what the cost is, and most importantly, how do you charge/discharge it safely?

While most of the batteries will be of the chemical variety, some mention will be made of mechanical batteries.

Lead acid, nickel metal, lipo, lithium iron, silicon carbon? With all the different battery types out there now, how can you be sure you're keeping it functioning at its best, and not creating a ticking time bomb?

This talk will cover the plethora of energy sources for off-grid radio operations and give tips for what works best and how to get the most out of it.

SpeakerBio: hamster

Passionate about electronics and energy storage



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Key Rotation Won't Save You: Hunting Workload Identity Backdoors in AWS and GCP

Tags: Cloud Village | Creator Talk/Panel

When: Saturday, Aug 8, 16:40 - 17:20 PDT

Where: LVCCW Level 3 W313 (Cloud Village Talks) - [Map](#)

Description:

Cloud incident response runbooks end with "rotate all keys and credentials." AWS IAM Roles Anywhere and GCP Workload Identity Federation were designed to remove keys from the trust chain, and that design is what lets an attacker survive standard containment.

This talk shows how an attacker registers their own certificate authority as an AWS Roles Anywhere trust anchor, or modifies a GCP Workload Identity Federation provider to trust an attacker-controlled identity, and mints fresh credentials indefinitely. Defender content has not caught up to the attack research: Roles Anywhere trust anchor and session events land in CloudTrail by default, but no published hunting query traces the CreateSession back to the issuing certificate authority via the hex serial recorded in roleSessionName. GCP pool and provider creation lands in Admin Activity logs for free, but the federated token exchange only lands in Data Access logs when explicitly enabled and paid for.

The session closes with the cross-cloud fingerprint: when the same attacker-controlled OIDC provider is registered in both clouds (as an AWS OIDC identity provider and as a GCP Workload Identity Federation pool provider), the same OIDC sub claim surfaces in both audit trails. Extracting and joining on it ties one attacker to two cloud incidents.

Attendees will gain the WIF Hunting Pack: a working playbook for keyless persistence in AWS and GCP, two prevention policy templates that block the attack at organization scope, and a cross-cloud correlation pattern for OIDC-based incident response. Live demo across speaker-controlled AWS and GCP environments. This talk is for blue teamers and platform security engineers who secure infrastructure across AWS and GCP.

SpeakerBio: Jie Wu

Jie is a Senior Security Engineer at Shopify based in New York City, working on cloud security, Kubernetes, and detection engineering to secure cloud infrastructure. She has spoken at KubeCon EU, fwd:cloudsec, and BSides (Chicago, Ottawa, Montréal), covering topics from Kubernetes security at scale to non-human identity accountability in the cloud. Before Shopify, she worked on cyber defense and vulnerability management at Bank of America.



[Return to Index](#) - Add to Google

- ics [Calendar](#) file

Title: Keychained Melody - Grabbing the Keys to the iCloud Kingdom

Tags: DEF CON Official Talk | Demo | Exploit

When: Friday, Aug 7, 11:00 - 11:59 PDT

Where: LVCCW Level 1 Hall 3 906 (Main Track 3) - [Map](#)

Description:

The Apple Keychain has become a cornerstone of credential management for millions of users across the Apple ecosystem. In response, Apple has implemented robust protections for the iCloud Keychain — restricting synchronization exclusively to devices within Apple’s “Circle of Trust” and encrypting stored secrets with keys protected by the Secure Enclave. These layered defenses are designed to ensure that even physical acquisition of Keychain data from Apple’s servers yields nothing actionable.

This talk introduces a novel vulnerability (CVE-2026-28860) that fundamentally undermines these protections. Leveraging a deep understanding of macOS internals, we demonstrate a technique capable of extracting all passwords stored within the Keychain — requiring neither root privileges, a user password, nor any prompts to the user. Beyond credential theft, we explore the broader attack surface this vulnerability exposes, presenting additional scenarios where data gleaned from the iCloud Keychain enables further, more severe compromise.

Speakers: Alex Radocea, Jaron Bradley

SpeakerBio: Alex Radocea

Founder of Supernetworks and cofounder of Longterm Security. Alex started in security pentesting financial firms on Wall Street at Matasano and cofounded RPISEC at RPI. He has worked on Apple's Product Security team, engineering at CrowdStrike, and Spotify's Security team. His research — presented at Black Hat and REcon — spans mobile messenger cryptography, kernel security, binary static analysis, and browser hardening, including the discovery of critical flaws in Apple's iCloud Keychain.

SpeakerBio: Jaron Bradley, Jamf

Jaron is the Director of Jamf Threat Labs where he focuses on discovering new ways to keep user's safe on Apple devices. He is author of the books "Threat Hunting macOS" and "OS X Incident Response". In his free time he manages themittenmac.com, a site dedicated to helping others learn security on the Apple ecosystem.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Keychecker : SSH Key based attack tool for DVCS Systems

Tags: Intro/Beginner | DEF CON Demo Labs | Defense/Blue Team | DevOps | Offense/Red Team | SecOps | DEF CON Demo Labs

When: Saturday, Aug 8, 13:00 - 13:45 PDT

Where: LVCCW Level 1 Hall 3 1003 (Demo Labs Track 3) - [Map](#)

Description:

KeyChecker is a CLI tool to fingerprint SSH private keys and identify which Git hosting accounts they unlock. In incident response and red team work, finding a private key is common, but scoping impact is slow and manual. KeyChecker automates the two primitives defenders and attackers both use: safe SSH handshakes that can reveal the mapped username, and read only git ls-remote probes that confirm whether a key can access a target repo.

The tool performs local key intelligence first, supporting OpenSSH, PEM, and DER formats, detecting key type (ed25519, rsa, ecdsa, dsa), key size, passphrase protection, fingerprints (SHA256 and MD5), and useful metadata from key comments. It then validates the key across multiple providers including GitHub, GitLab, Bitbucket, Codeberg, Gitea, and Hugging Face, extracting usernames where possible, and optionally using a GitHub token for organization discovery.

KeyChecker also supports repository discovery with a wordlist and configurable concurrency, giving a clear blast radius report like “this key unlocks these private repositories.” It is designed for authorized assessments, runs locally, and avoids write operations.

SpeakerBio: Anant Shrivastava

Anant Shrivastava is the founder of Cyfinoid Research and a long time offensive security practitioner with a focus on application, cloud, and supply chain security. He has delivered trainings and talks at Black Hat (USA, Europe, Asia), Nullcon, c0c0n, BSides, Rootconf and multiple other events, and runs projects such as Hacking Archives of India to highlight real work from the security community. His courses are built from real consulting and red team experience, with an emphasis on attack chains that actually show up in the field and defenses that teams can implement the next day.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Keychecker : SSH Key based attack tool for DVCS Systems

Tags: Intro/Beginner | DEF CON Demo Labs | Defense/Blue Team | DevOps | Offense/Red Team | SecOps | DEF CON Demo Labs

When: Saturday, Aug 8, 12:00 - 12:45 PDT

Where: LVCCW Level 1 Hall 3 1003 (Demo Labs Track 3) - [Map](#)

Description:

KeyChecker is a CLI tool to fingerprint SSH private keys and identify which Git hosting accounts they unlock. In incident response and red team work, finding a private key is common, but scoping impact is slow and manual. KeyChecker automates the two primitives defenders and attackers both use: safe SSH handshakes that can reveal the mapped username, and read only git ls-remote probes that confirm whether a key can access a target repo.

The tool performs local key intelligence first, supporting OpenSSH, PEM, and DER formats, detecting key type (ed25519, rsa, ecdsa, dsa), key size, passphrase protection, fingerprints (SHA256 and MD5), and useful metadata from key comments. It then validates the key across multiple providers including GitHub, GitLab, Bitbucket, Codeberg, Gitea, and Hugging Face, extracting usernames where possible, and optionally using a GitHub token for organization discovery.

KeyChecker also supports repository discovery with a wordlist and configurable concurrency, giving a clear blast radius report like “this key unlocks these private repositories.” It is designed for authorized assessments, runs locally, and avoids write operations.

SpeakerBio: Anant Shrivastava

Anant Shrivastava is the founder of Cyfinoid Research and a long time offensive security practitioner with a focus on application, cloud, and supply chain security. He has delivered trainings and talks at Black Hat (USA, Europe, Asia), Nullcon, c0c0n, BSides, Rootconf and multiple other events, and runs projects such as Hacking Archives of India to highlight real work from the security community. His courses are built from real consulting and red team experience, with an emphasis on attack chains that actually show up in the field and defenses that teams can implement the next day.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Keynote: Colorado's Creation of RLAs

Tags: Voting Village | Creator Talk/Panel

When: Saturday, Aug 8, 12:00 - 12:45 PDT

Where: LVCCW Level 2 W220 (Voting Village) (Voting Village Talks) - [Map](#)

Description:

As Colorado's 38th Secretary of State, Mr. Williams oversaw the creation of the nation's first full forensic risk limiting audit ("RLA") in 2017.

Colorado's legislature ordered the use of RLA's in 2009 -- long before widespread media coverage of fears about hacking election equipment and interference by foreigners or other bad actors. Three Secretaries of State later, Colorado implemented the nation's first full RLA in 2017.

An RLA is a procedure that provides strong statistical evidence that the election outcome is right and has a high probability of correcting a wrong outcome. Risk-limiting audits require human beings to examine and verify more ballots in close races (exactly when you want to examine more ballots), and fewer ballots in races with wide margins.

Colorado's process attracted attention nationwide. The Washington Post pronounced Colorado "the safest state to cast a vote." Matt Masterson, then chairman of the U.S. Election Assistance Commission, attended the implementation and stated that "Colorado is a national leader in exploring innovative solutions for accessible, secure and auditable elections."

Secretary Williams will discuss the benefits of RLAs, the processes used, and some of the hurdles Colorado overcame during its implementation.

SpeakerBio: Wayne Williams

Wayne Williams served as Colorado's 38th Secretary of State from 2015 to 2019 and now serves as Colorado Springs Chief of Staff for Mayor Yemi Mobolade. Secretary Williams' 20 years of elected service includes four years as Clerk and Recorder for Colorado's most populous county. He continues to serve as a designated election official and on the Board of Advisors for Verified Voting.

As Secretary of State, Wayne Williams adopted rules requiring voter-verifiable paper ballots, created the nation's first full risk limiting audit, and defended Colorado voters against attempts by rogue electors to deprive them of their vote in the 2016 presidential election. Secretary Williams' actions were upheld by a unanimous U.S. Supreme Court.

His work in these positions earned regional and national recognition, including the National Association of Secretaries of State Medallion Award, the Colorado League of Women Voters' Leader of Democracy, Defender of Democracy, and the Truman Foundation's Stevens Award for attorneys in public service. He has been appointed to state boards by Colorado Governors from both political parties.

Secretary Williams received his B.A. in Political Science from BYU (1986), and his J.D. from the University of Virginia Law School (1989).

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Killing AI Slop: A Multi-Model Orchestration Framework That Only Reports Findings It Can Prove

Tags: Bug Bounty Village | Creator Talk/Panel

When: Saturday, Aug 8, 12:00 - 12:30 PDT

Where: LVCCW Level 1 Hall 3 1102 (Creator Stage 6) - [Map](#)

Description:

AI-assisted bug hunting has a reliability problem. Modern models can generate convincing vulnerability reports, but many fail under validation. They reference non-existent endpoints, unreachable exploit paths, or attack chains that break when tested against the target. As a result, triage teams spend increasing time reviewing low-quality submissions, while researchers struggle to separate genuine vulnerabilities from model-generated noise. This talk presents a multi-agent bug hunting framework built around a simple principle: a finding is not considered valid until it has been reproduced against the target. The goal is to improve the quality and reliability of reported findings. The process begins with understanding the target. Before testing starts, the framework analyzes JavaScript, API specifications, documentation, authentication flows, endpoints, parameters, and technologies to build a structured model of the application. This enables agents to reason about the actual attack surface rather than relying on assumptions. An orchestrator coordinates specialized agents operating from a shared understanding of the target. Candidate findings are routed through a central coordination layer that manages context sharing and eliminates duplicate results. To improve decision-making and reduce hallucinations, the agents leverage a RAG engine backed by publicly disclosed vulnerability reports and security research. Every candidate finding passes through a verification stage that evaluates application-specific context, observed behavior, and supporting evidence. Findings that pass validation are further tested to determine their maximum practical impact before being reported, while non-actionable and expected behavior is discarded. The presentation covers the architecture, orchestration model, and verification workflow, providing practical guidance for building AI-assisted security tooling that prioritizes evidence over assumptions.

SpeakerBio: Armaan Pathan

Armaan Pathan is a Senior Security Engineer at KATIM with more than 10 years of experience in offensive security, application security, and vulnerability research, helping organizations identify and remediate critical security risks. Throughout his career, he has discovered and responsibly disclosed vulnerabilities impacting major companies, including Google, Meta, and Apple, through bug bounty and coordinated vulnerability disclosure programs. His interests include web and API security, security engineering, and exploring how AI can be used to enhance offensive security and vulnerability research. Armaan actively contributes to the security community-publishing technical blogs, presenting at conferences, and raising awareness of emerging threats and practical defenses.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Noob Community - Friday - 10:00-17:59 PDT

Title: Kryptsec Labs

Tags: Noob Community | Creator Event/Activity

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 4 1417 (Noob Community) - [Map](#)

Description:

Kryptsec started as a Discord server for people who wanted to learn cybersecurity together and has grown into a company focused on making security training engaging rather than monotonous, including hands-on, AI-assisted CTF labs and OASIS, its open-source tool for benchmarking AI agent vulnerabilities. Stop by the Kryptsec Labs table during village hours to work through their hands-on challenges.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Noob Community - Saturday - 10:00-17:59 PDT

Title: Kryptsec Labs

Tags: Noob Community | Creator Event/Activity

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 4 1417 (Noob Community) - [Map](#)

Description:

Kryptsec started as a Discord server for people who wanted to learn cybersecurity together and has grown into a company focused on making security training engaging rather than monotonous, including hands-on, AI-assisted CTF labs and OASIS, its open-source tool for benchmarking AI agent vulnerabilities. Stop by the Kryptsec Labs table during village hours to work through their hands-on challenges.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Noob Community - Sunday - 10:00-13:59 PDT

Title: Kryptsec Labs

Tags: Noob Community | Creator Event/Activity

When: Sunday, Aug 9, 10:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 4 1417 (Noob Community) - [Map](#)

Description:

Kryptsec started as a Discord server for people who wanted to learn cybersecurity together and has grown into a company focused on making security training engaging rather than monotonous, including hands-on, AI-assisted CTF labs and OASIS, its open-source tool for benchmarking AI agent vulnerabilities. Stop by the Kryptsec Labs table during village hours to work through their hands-on challenges.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Scambait Village - Friday - 10:00-17:59 PDT

Title: KSCM Scambait Radio

Tags: Scambait Village | Creator Event/Activity

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 208 (Scambait Village) - [Map](#)

Description:

Prerecorded scambait calls running in Discord voice throughout the day. Bring earbuds and tune in from your phone while you walk the village or the rest of the con. Listen to real interactions, hear how experienced baiters handle different situations, and pick up new techniques and banter styles. Ambient and educational, drop in for a few minutes or stay for a whole set.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Scambait Village - Saturday - 10:00-17:59 PDT

Title: KSCM Scambait Radio

Tags: Scambait Village | Creator Event/Activity

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 208 (Scambait Village) - [Map](#)

Description:

Prerecorded scambait calls running in Discord voice throughout the day. Bring earbuds and tune in from your phone while you walk the village or the rest of the con. Listen to real interactions, hear how experienced baiters handle different situations, and pick up new techniques and banter styles. Ambient and educational, drop in for a few minutes or stay for a whole set.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Scambait Village - Sunday - 10:00-15:59 PDT

Title: KSCM Scambait Radio

Tags: Scambait Village | Creator Event/Activity

When: Sunday, Aug 9, 10:00 - 15:59 PDT

Where: LVCCW Level 1 Hall 1 208 (Scambait Village) - [Map](#)

Description:

Prerecorded scambait calls running in Discord voice throughout the day. Bring earbuds and tune in from your phone while you walk the village or the rest of the con. Listen to real interactions, hear how experienced baiters handle different situations, and pick up new techniques and banter styles. Ambient and educational, drop in for a few minutes or stay for a whole set.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

The Diana Initiative - Saturday - 12:00-12:10 PDT

Title: Kubernetes CTF at DEF CON Contest Tour

Tags: The Diana Initiative | Creator Tour

When: Saturday, Aug 8, 12:00 - 12:10 PDT

Where: LVCCW Level 1 South Lobby / Atrium - [Map](#)

Description:

Interested in visiting Kubernetes CTF at DEF CON Contest but afraid to go by yourself? The Diana Initiative is hosting tours! Follow a volunteer to Kubernetes CTF at DEF CON Contest and be introduced to the community and activities inside!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Contests - Friday - 10:00-17:59 PDT

Title: Kubernetes CTF

Tags: Kubernetes CTF | Contest

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 212 (Kubernetes CTF) - [Map](#)

Description:

Want to learn more about Kubernetes hacking or compete against other people in a Capture the Flag contest? Sign up on-line and come see us in person/on Discord at the Kubernetes Capture the Flag (CTF) contest .

We have two events - you can play in both if you like.

From Friday to Sunday, we have a non-competitive Learning CTF, where you can go through last year's Kubernetes CTF scenario, referring to a cheat sheet whenever you want. This runs from Friday 12:00 to Sunday 12:00. We'll be in the contest area to support you during:

Friday: 12:00-17:00 Saturday: 10:00-17:00 Sunday: 10:00-12:00

On Saturday only, you can play in the competitive Kubernetes CTF challenge, where teams (of one or more) can build and test their skills. Each team is given access to a single Kubernetes cluster that contains a set of challenges. This runs from 10:30am to 5:30pm on Saturday.

Find out more and sign up at: <https://containersecurityctf.com/>

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Contests - Sunday - 10:00-11:59 PDT

Title: Kubernetes CTF

Tags: Kubernetes CTF | Contest

When: Sunday, Aug 9, 10:00 - 11:59 PDT

Where: LVCCW Level 1 Hall 1 212 (Kubernetes CTF) - [Map](#)

Description:

Want to learn more about Kubernetes hacking or compete against other people in a Capture the Flag contest? Sign up on-line and come see us in person/on Discord at the Kubernetes Capture the Flag (CTF) contest .

We have two events - you can play in both if you like.

From Friday to Sunday, we have a non-competitive Learning CTF, where you can go through last year's Kubernetes CTF scenario, referring to a cheat sheet whenever you want. This runs from Friday 12:00 to Sunday 12:00. We'll be in the contest area to support you during:

Friday: 12:00-17:00 Saturday: 10:00-17:00 Sunday: 10:00-12:00

On Saturday only, you can play in the competitive Kubernetes CTF challenge, where teams (of one or more) can build and test their skills. Each team is given access to a single Kubernetes cluster that contains a set of challenges. This runs from 10:30am to 5:30pm on Saturday.

Find out more and sign up at: <https://containersecurityctf.com/>

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Contests - Saturday - 10:00-17:59 PDT

Title: Kubernetes CTF

Tags: Kubernetes CTF | Contest

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 212 (Kubernetes CTF) - [Map](#)

Description:

Want to learn more about Kubernetes hacking or compete against other people in a Capture the Flag contest? Sign up on-line and come see us in person/on Discord at the Kubernetes Capture the Flag (CTF) contest .

We have two events - you can play in both if you like.

From Friday to Sunday, we have a non-competitive Learning CTF, where you can go through last year's Kubernetes CTF scenario, referring to a cheat sheet whenever you want. This runs from Friday 12:00 to Sunday 12:00. We'll be in the contest area to support you during:

Friday: 12:00-17:00 Saturday: 10:00-17:00 Sunday: 10:00-12:00

On Saturday only, you can play in the competitive Kubernetes CTF challenge, where teams (of one or more) can build and test their skills. Each team is given access to a single Kubernetes cluster that contains a set of challenges. This runs from 10:30am to 5:30pm on Saturday.

Find out more and sign up at: <https://containersecurityctf.com/>

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Hackers.town - Saturday - 12:00-12:30 PDT

Title: KYC and XMR... FOR HACKERS!

Tags: Hackers.town | Creator Talk/Panel

When: Saturday, Aug 8, 12:00 - 12:30 PDT

Where: LVCCW Level 1 Hall 3 1100 (Creator Stage 7) - [Map](#)

Description:

An overview of handy usecases for specific crypto currencies for technologists.

SpeakerBio: AltKey

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: L.A.Y.E.R.S - Layered Analysis Engine for Browser Extension Risk and Security

Tags: DEF CON Demo Labs | Intermediate | AppSec | Offense/Red Team | DEF CON Demo Labs

When: Friday, Aug 7, 14:00 - 14:45 PDT

Where: LVCCW Level 1 Hall 3 901 (Demo Labs Track 5) - [Map](#)

Description:

Browser Extensions is one of the overlooked attack surface in the modern era. Most browser extension have permissions to allow direct access to cookies, browsing history, network requests and a poorly written extension can help attackers with stuff like silently steal credentials, log keystrokes, fingerprint users etc.

L.A.Y.E.R.S. (Logical Analyst for Your Extension Risk Surface) is a fully client-side chrome browser extension security engine that performs multi-layered security analysis on extensions. The tool performs analysis on various levels like JS analysis, permissions analysis, manifest analysis, secret scanning, URL extractions etc. simultaneously to uncover potential risks. The tool comes with its own scoring system guiding the team if the extension is safe to use or not.

L.A.Y.E.R.S. is designed for security researchers auditing in-house extensions, third-party extensions, red teams assessing browser attack surfaces, enterprises enforcing extension policies, and developers seeking to harden their own extensions before publication.

What sets L.A.Y.E.R.S. apart begins with its privacy-first architecture - the entire analysis runs in-browser via the File System API and JSZip, with very little setup required. On the detection side, it incorporates Shannon entropy analysis. To keep results actionable rat

Speakers: Abhinav Khanna, Krishna Chaganti

SpeakerBio: Abhinav Khanna

Abhinav is an Information Security Professional with 7+ years of experience and currently works at S&P Global. His area of expertise include Web App Security, API Security, Mobile App Security, Secure Architecture. He has spoken at conferences like BlackHat USA, DefCon 33, BlackHat Europe, BlackHat Asia etc.

SpeakerBio: Krishna Chaganti

Krishna Chaganti works as Associate Director Application Security at S&P Global, based in the USA, with over a decade of experience in Information Security. As a Certified Information Security Manager (CISM), he leads a team of more than 10 pentesters and specializes in Application Security along with Security Architecture.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: L.A.Y.E.R.S - Layered Analysis Engine for Browser Extension Risk and Security

Tags: DEF CON Demo Labs | Intermediate | AppSec | Offense/Red Team | DEF CON Demo Labs

When: Saturday, Aug 8, 13:00 - 13:45 PDT

Where: LVCCW Level 1 Hall 3 901 (Demo Labs Track 5) - [Map](#)

Description:

Browser Extensions is one of the overlooked attack surface in the modern era. Most browser extension have permissions to allow direct access to cookies, browsing history, network requests and a poorly written extension can help attackers with stuff like silently steal credentials, log keystrokes, fingerprint users etc.

L.A.Y.E.R.S. (Logical Analyst for Your Extension Risk Surface) is a fully client-side chrome browser extension security engine that performs multi-layered security analysis on extensions. The tool performs analysis on various levels like JS analysis, permissions analysis, manifest analysis, secret scanning, URL extractions etc. simultaneously to uncover potential risks. The tool comes with its own scoring system guiding the team if the extension is safe to use or not.

L.A.Y.E.R.S. is designed for security researchers auditing in-house extensions, third-party extensions, red teams assessing browser attack surfaces, enterprises enforcing extension policies, and developers seeking to harden their own extensions before publication.

What sets L.A.Y.E.R.S. apart begins with its privacy-first architecture - the entire analysis runs in-browser via the File System API and JSZip, with very little setup required. On the detection side, it incorporates Shannon entropy analysis. To keep results actionable rat

Speakers: Abhinav Khanna, Krishna Chaganti

SpeakerBio: Abhinav Khanna

Abhinav is an Information Security Professional with 7+ years of experience and currently works at S&P Global. His area of expertise include Web App Security, API Security, Mobile App Security, Secure Architecture. He has spoken at conferences like BlackHat USA, DefCon 33, BlackHat Europe, BlackHat Asia etc.

SpeakerBio: Krishna Chaganti

Krishna Chaganti works as Associate Director Application Security at S&P Global, based in the USA, with over a decade of experience in Information Security. As a Certified Information Security Manager (CISM), he leads a team of more than 10 pentesters and specializes in Application Security along with Security Architecture.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: La Rosa de Guadalupe DFIR: Serie de 3 capítulos de misterio Cyber*

Tags: La Villa Community | Creator Talk/Panel

When: Sunday, Aug 9, 11:30 - 11:59 PDT

Where: LVCCW Level 1 Hall 4 1416 (La Villa Community) Main Stage - [Map](#)

Description:

Tres insólitos incidentes de ciberseguridad fueron resueltos por dos investigadores en Incidentes de Ciberseguridad con ayuda de múltiples técnicas de "sniper-forensics" y una "Rosa Blanca" les confirmó sus sospechas iniciales y los llevó a encontrar la verdad.

Se abordará el análisis detallado de las diferentes fuentes de información (bitácoras, artefactos y contexto).

Speakers: Victor Gomez, Horacio Bazán

SpeakerBio: Victor Gomez, DFIR Principal

Victor Gomez is a cybersecurity professional coming from the sysadmin-architecture world. He has focused his career on digital forensics, incident response, and Intel, responding to all kinds of attacks on multiple and different sizes of organizations & industries and leading multiple Cyber* teams. In his spare time, he likes to mentor and organize a local meetup in Mexico City.

SpeakerBio: Horacio Bazán, DFIR Principal

Ph.D. in Computer Sciences (cybersecurity & AI) from Instituto Politécnico Nacional (National Polytechnic Institute, IPN) in 2024. For the past few years, I have been working as an Incident Responder, taking on multiple roles in cybersecurity. My professional interests include incident response, Artificial Intelligence (AI) applied to Cybersecurity, primarily in Android malware analysis and Computer Forensics.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

La Villa Community - Sunday - 13:00-13:30 PDT

Title: La Villa - Closing Ceremony (ESP)

Tags: La Villa Community | Creator Talk/Panel

When: Sunday, Aug 9, 13:00 - 13:30 PDT

Where: LVCCW Level 1 Hall 4 1416 (La Villa Community) Main Stage - [Map](#)

Description:



[Return to Index](#) - Add to Google - ics [Calendar](#) file

La Villa Community - Friday - 10:00-10:30 PDT

Title: La Villa - Opening Ceremony (ESP)

Tags: La Villa Community | Creator Talk/Panel

When: Friday, Aug 7, 10:00 - 10:30 PDT

Where: LVCCW Level 1 Hall 4 1416 (La Villa Community) Main Stage - [Map](#)

Description:



[Return to Index](#) - Add to Google - ics [Calendar](#) file

The Diana Initiative - Friday - 13:50-13:59 PDT

Title: La Villa Tour

Tags: The Diana Initiative | Creator Tour

When: Friday, Aug 7, 13:50 - 13:59 PDT

Where: LVCCW Level 1 South Lobby / Atrium - [Map](#)

Description:

Interested in visiting La Villa but afraid to go by yourself? The Diana Initiative is hosting tours! Follow a volunteer to La Villa and be introduced to the community and activities inside!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Data Duplication Village - Sunday - 10:00-10:59 PDT

Title: Last chance to pick up drives at the DDV

Tags: Data Duplication Village | Creator Event/Activity

When: Sunday, Aug 9, 10:00 - 10:59 PDT

Where: LVCCW Level 2 W203 (Data Duplication Village) - [Map](#)

Description:

This is your last chance to pickup your drives whether they're finished or not. Get here between 10:00am and 11:00am on Sunday as any drives left behind are considered donations.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Latest News in the Proxmark World

Tags: Radio Frequency Village | Creator Talk/Panel

When: Friday, Aug 7, 17:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 3 1102 (Creator Stage 6) - [Map](#)

Description:

A whirlwind tour of the latest developments in the Proxmark ecosystem, from new hardware announcements and firmware releases. We'll explore what's new in the RFID security landscape, highlight recent innovations from the community, and take a look at where the Proxmark platform is headed next. Whether you're a long-time user or just getting started, this session will bring you up to speed on the most important updates from the Proxmark world.

SpeakerBio: Iceman

Christian Herrmann – RFID Hacker | Co-Founder of AuroraSec & RRG | MCPD Enterprise Architect

Christian Herrmann, better known in the hacker community as “Iceman”, is a co-founder of AuroraSec and RRG, and has helped develop many of today's most widely used RFID research tools, including the Proxmark3 RDV4 and the Chameleon Mini.

He is a well-known RFID hacking and Proxmark3 evangelist, serving the community as both a forum administrator and a major code contributor alongside other developers since 2013. Christian has spoken at hacker conferences around the world, including BalcCon, WHY-2025, Troopers, Black Hat Asia, DEF CON, Hardwear IO, SSTIC, NullCon, Pass-the-Salt, BSides Tallinn, BlackAlps, and SaintCon.

He also runs a YouTube channel where he shares his knowledge of RFID hacking with the public.

With over 14 years of experience in bespoke software development, Christian specializes in .NET platforms and is a Certified MCPD Enterprise Architect.

He possesses near-unmatched expertise in the Proxmark3 architecture and various RFID technologies.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

La Villa Community - Saturday - 17:30-18:30 PDT

Title: latinas.exe has entered the chat (ESP - POR)

Tags: La Villa Community | Creator Talk/Panel

When: Saturday, Aug 8, 17:30 - 18:30 PDT

Where: LVCCW Level 1 Hall 4 1416 (La Villa Community) Main Stage - [Map](#)

Description:



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: LaunchBreak: a Sip of Tea, a Click, and a Full Multi-stage Desktop Takeover

Tags: DEF CON Official Talk | Demo | Tool | Exploit

When: Sunday, Aug 9, 11:00 - 11:59 PDT

Where: LVCCW Level 1 Hall 3 1006 (Main Track 1) - [Map](#)

Description:

As AI and agentic desktop apps rapidly adopt custom URI schemes for one-click onboarding—MCP install, plugin install, configuration import, prompt-driven actions—a browser click becomes a gateway into privileged local logic. Prior Electron research assumes the attacker is already inside the app; the browser-triggered, end-to-end exploitation model has remained unexplored.

We present LaunchBreak: a class of vulnerabilities where a crafted browser link launches a desktop app and injects attacker-controlled input into a multi-stage, multi-process exploit chain. We systematize the attack surface across three dimensions: payload sources (URI, attacker server, local file), cross-process flows (main/utility/renderer), and sinks (command exec, dynamic eval, module loading).

Our findings include 18 zero-days, 17 of them full RCEs, with 11 CVEs and a bug bounty. The affected apps include AFFiNE (60k stars, CVE-2026-21853), Hyper (Vercel's terminal, bounty awarded), Cherry Studio (CVE-2025-54063), Pinokio (CVE-2025-44109), deepchat (CVE-2025-55733), Paperlib (CVE-2025-64743), and more, spanning AI assistants, music players, and dev tools. We'll demo live exploits against apps, walk through the chains, and release Proton, the agent-guided segmented fuzzing framework we built to find them, plus PoCs for every vulnerability.

The related CCS paper if that submission is accepted (the result comes out in June.), if not, then none.

Speakers: Gavin Zhong, Zhengyu Liu, Jianjia Yu

SpeakerBio: Gavin Zhong, Johns Hopkins University

Jiacheng (Gavin) Zhong is a security researcher, focusing on AI system security, program analysis, and identity security. He recently completed his M.S. in Security Informatics at Johns Hopkins University, where his work was accepted to IEEE S&P 2026. Gavin has reported over 30 CVEs in widely used open-source projects. He is also an active CTF player with r3kapiG, an international team ranked top 3 worldwide.

SpeakerBio: Zhengyu Liu, Johns Hopkins University

Zhengyu Liu is a third-year PhD student in Computer Science at Johns Hopkins University. His research focuses on web and software security via program analysis. His work received Distinguished Paper (S&P '25), Honorable Mention (USENIX '25), and Best Student Paper (ICICS '22). He is a DEF CON speaker and is a member of CTF team TheHackersCrew.

SpeakerBio: Jianjia Yu, Johns Hopkins University

Jianjia Yu is a PhD student at Johns Hopkins University, advised by Prof. Yinzhi Cao. Her research focuses on security and privacy in web and mobile ecosystems using program analysis techniques. Her work has received Distinguished Paper Awards at CCS '23 and S&P '25, and an Honorable Mention at USENIX Security '25. She has discovered over 40 zero-day vulnerabilities and uncovered privacy leaks affecting millions of users across browser extensions and mobile applications.



Social Gatherings/Events - Friday - 19:00-21:59 PDT

Title: Lawyers Meet

Tags: Meetup

When: Friday, Aug 7, 19:00 - 21:59 PDT

Where: LVCCW Level 3 W301 (Misc Meeting Room) - [Map](#)

Description:

If you're a lawyer (recently unfrozen or otherwise), a judge or a law student please make a note to join Jeff McNamara for a friendly get-together, drinks, and conversation.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Learning Deception by Doing: Attacking and Defending

Tags: La Villa Community | Creator Talk/Panel

When: Saturday, Aug 8, 10:00 - 10:30 PDT

Where: LVCCW Level 1 Hall 4 1416 (La Villa Community) Main Stage - [Map](#)

Description:

Cyber deception is one of the most powerful and least understood defensive disciplines — most practitioners have read about honeypots, but few have ever deployed a breadcrumb, watched an attacker chase a fake credential, or felt the confusion deception causes from the attacker's side.

This session shares the fundamentals of deception by doing and experiencing: what deceptive artifacts exist (honey-credentials, deceptive configs, honey-services, synthetic activity), where they belong in a real environment, what telemetry they generate, and how they change an adversary's behavior. Everything is practiced in an open-source, Docker-based playground that recreates a realistic multi-tier company — with an attacker toolkit on one side and a defender SIEM on the other — so attendees can safely play both roles.

The 25-minute format is a guided demo; the 50-minute format is a hands-on lab.

Speakers: Diego Staino, Fede Pacheco

SpeakerBio: Diego Staino, R&D+i Manager

Cybersecurity professional with 15+ years of experience as Security and IT consultant. Certified Incident Handler (ECIH) with a degree in Information Security and Communications. Currently works as R&D+i Manager at BASE4 Security, where he leads the company's research and development initiatives.

SpeakerBio: Fede Pacheco, Cybersecurity Services Director, BASE4 Security

Especialista en ciberseguridad con formación en ingeniería electrónica, y destacadas certificaciones profesionales en seguridad de la información. Cuenta con 20 años de experiencia docente, principalmente en la Universidad Tecnológica Nacional. Lleva publicados cuatro libros y diversos trabajos de investigación en temáticas de ciberseguridad y de educación, algunos de los cuales han sido presentados en congresos y conferencias globales. Además, se desempeñó en roles de liderazgo de alcance regional en distintas empresas multinacionales. Actualmente tiene a cargo el área de Cybersecurity Services de BASE4 Security.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Legally Hacked: how countries decide when security research Is allowed

Tags: Policy @ DEF CON | Creator Talk/Panel

When: Friday, Aug 7, 16:30 - 16:59 PDT

Where: LVCCW Level 1 Hall 3 801 (Creator Stage 1) - [Map](#)

Description:

As governments increasingly rely on vulnerability disclosure to secure digital systems, many security researchers still operate under cybercrime laws that criminalise the very activity those frameworks depend on. This talk offers a fast paced, global comparison of how different countries are addressing that paradox. Drawing on recent reforms and live policy debates, it introduces a practical taxonomy of legal protection models—from statutory defences to prosecutorial guidance and vulnerability disclosure policies as authorisation—and examines their real world implications for researchers. The session concludes with a concise “Minimum Viable Safe Harbour” checklist, highlighting the core principles needed to protect good faith security research while preventing abuse.

SpeakerBio: Katharina "Kat S" Sommer, NCC Group

Kat is a seasoned policy and strategy leader with over 15 years of experience spanning political institutions, consultancy, and corporate roles. At NCC Group, she has built and scaled the Government Affairs and Analyst Relations functions, embedding them as strategic enablers of the company’s mission to create a more secure digital future. Her work has shaped cyber policy debates across the UK, EU, and globally—most notably through her leadership in the CyberUp Campaign and contributions to initiatives such as the UN’s Cybercrime Convention and the UK-France Pall Mall Process. Kat is a passionate advocate for cyber resilience, known for her ability to convene diverse stakeholders, drive regulatory engagement, and deliver tangible business outcomes. She holds a Master’s in Public Affairs & Lobbying from Brunel University and a Bachelor’s in Public Administration with a focus on European Studies. Outside of work, she is a 4th Dan black belt in Tae Kwon Do.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Malware Village - Saturday - 15:20-16:05 PDT

Title: Leigh Trinity OTW

Tags: Malware Village | Creator Talk/Panel

When: Saturday, Aug 8, 15:20 - 16:05 PDT

Where: LVCCW Level 1 Hall 2 600 (Malware Village) Talks - [Map](#)

Description:

Discussion on the current state of cellphone and network hacking.

SpeakerBio: Leigh Gilbert, Malware village

Leigh Trinity is a Canadian exploit developer, red team hacker, and instructor known for her work in binary exploitation and reverse engineering. Now branching out into malware development.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Lessons from a decade of building whistleblower tech

Tags: DEF CON Official Talk | Tool

When: Friday, Aug 7, 14:00 - 14:59 PDT

Where: LVCCW Level 1 Hall 3 906 (Main Track 3) - [Map](#)

Description:

Internet pioneer Aaron Swartz's last project was SecureDrop, a whistleblower submission system that can be used by news outlets and whistleblowers to communicate safely online. At the time of Aaron's tragic death, SecureDrop was just a prototype, but it's now run by Freedom of the Press Foundation and used by dozens of the biggest news outlets around the world. This talk will explore the unique technical challenges in running an anonymous whistleblower platform, the future of whistleblowing technology, and the lessons we have learned about how whistleblowers and journalists actually communicate along the way. In addition, we will preview our new project, a collaboration with the Tor Project called WEBCAT, which aims to solve code verification on web browsers and make end-to-end encryption for web applications safer.

<https://securedrop.org> <https://webcat.tech>

Speakers: Trevor Timm, redshiftzero

SpeakerBio: Trevor Timm, Freedom of the Press Foundation

Trevor is a co-founder and the executive director of Freedom of the Press Foundation (FPF), and has served on its board since 2012. He is a journalist, activist, and legal analyst whose writing has appeared in The New York Times, The Guardian, USA Today, The Atlantic, Al Jazeera, Foreign Policy, Harvard Law & Policy Review, and Politico. Trevor formerly worked as an activist at the Electronic Frontier Foundation. Before that, he helped the longtime general counsel of The New York Times, James Goodale, write the book, "Fighting for the Press," on the Pentagon Papers and the First Amendment. He received his J.D. from New York Law School. In 2013, he received the Hugh Hefner First Amendment Award for journalism.

SpeakerBio: redshiftzero, Freedom of the Press Foundation

Jennifer is the chief technology officer at Freedom of the Press Foundation (FPF), where she oversees the organization's engineering teams. She is an engineer, researcher, and cypherpunk. Prior to this role, she was a founding engineer at Penumbra Labs, focusing on applied cryptography for privacy-preserving payments. She previously led development for the SecureDrop whistleblower platform. She also co-founded Lucy Parsons Labs, a Chicago-based civil liberties group. Jennifer has spoken at events including Hackers on Planet Earth, USENIX Enigma, and DEF CON Crypto & Privacy Village. She holds a doctorate in astrophysics from the University of Chicago.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Noob Community - Friday - 15:30-15:45 PDT

Title: Lessons Learned From A Decade of Resumes

Tags: Noob Community | Creator Talk/Panel

When: Friday, Aug 7, 15:30 - 15:45 PDT

Where: LVCCW Level 1 Hall 4 1417 (Noob Community) - [Map](#)

Description:

After having reviewed resumes for the last decade in a variety of industries (although chiefly cybersecurity), I have a few things to say!

Want to learn how to craft a compelling resume? Want to know what to avoid? This session aims to help jobseekers sell themselves better.

Not only will I dive into the dos and don'ts of resume success, but I will also cover LinkedIn, interviews, networking, and other relevant topics.

If you're looking for work in this brutal market, I hope I can help you out.

SpeakerBio: Britt Kemp

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

DEF CON Groups - Sunday - 10:00-10:30 PDT

Title: Lessons Learned from Building a New DEF CON Group presented by DC724

Tags: DEF CON Groups | Creator Talk/Panel

When: Sunday, Aug 9, 10:00 - 10:30 PDT

Where: LVCCW Level 1 Hall 3 1100 (Creator Stage 7) - [Map](#)

Description:

Building a new DEF CON Group comes with a lot of trial, error, and unexpected lessons. DC724 will share real-world experience from the early stages of growing a newer group, including finding space, building relationships, coordinating with other communities, avoiding common mistakes, and creating momentum. This session is especially useful for newer POCs, prospective organizers, and anyone trying to get a local hacker community off the ground.

Speakers:Cliff "GritsnGravy" Friedel,Joe "jbohack"

SpeakerBio: Cliff "GritsnGravy" Friedel, DC 724

Cliff Friedel (GritsnGravy) is one of the co-founders of DC 724 and has been working with computers and technology since 1979. Working in various IT disciplines from the 1980s until today, Grits has got his hands into everything from BBSes to ISPs to storage acceleration networks. Now semi-retired, he focuses on retro computers, making nerdy T-shirts, RF technologies and amateur radio, and occasionally trying to throw a god roll at the craps tables.

SpeakerBio: Joe "jbohack", DC 724/Nyan Devices

Joe Buhagiar (jbohack) is a Security Engineer at NaviSec, specializing in incident response and penetration testing. He is also the Co-Founder and Lead Developer of Nyan Devices, the creators of the nyanBOX, a wireless security toolkit covering Wi-Fi, Bluetooth, and RF, with a focus on device visibility and counter-surveillance research. He is a Co-Founder of DC724.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Lessons Learned from Poland and Beyond: The State of Electric Sector Attacks in 2025

Tags: ICS Village | Creator Talk/Panel

When: Friday, Aug 7, 17:00 - 17:30 PDT

Where: LVCCW Level 1 Hall 3 801 (Creator Stage 1) - [Map](#)

Description:

2026 featured news of a new attempted, disruptive cyber attack against the electric sector. Instead of transmission or distribution in Ukraine, however, the event focused on generating assets in Poland. Irrespective of impact, the very fact such an action was attempted is concerning and newsworthy. However, the details of the event demonstrate the state of the "now" for electric sector events, in terms of their successes as well as failures.

In this discussion we will leverage all available public reporting to look at where the attackers innovated, borrowed from past events, and failed to learn from history in the December 2025 Polish event. From this discussion we will set the incident in context of both concurrent intrusions, such as Volt Typhoon activity, and historical incidents, linked to the Sandworm threat actor, to see just where adversaries are today with respect to tradecraft and sector knowledge.

From this exploration, attendees will emerge with a better understanding of what adversaries are "getting right" about such events, and where they still fall short. Furthermore, review of events will show the significance of physical safeguards and controls in ensuring continuous operations in the face of cyber effects, and how adversaries remain challenged to overcome such barriers.

SpeakerBio: Joe Slowik, Dataminr

Joe Slowik has over 15 years of experience across multiple cyber domains, ranging from offensive operations through incident response to threat intelligence and research. Currently, Joe serves as director of cybersecurity alerting strategy at Dataminr, but has previously held various roles at organizations such as Huntress, DomainTools, the MITRE Corporation, and Los Alamos National Laboratory.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Let's BLESPl0.it the world together - introducing a new portable Bluetooth Low Energy security tool

Tags: Radio Frequency Village | Creator Talk/Panel

When: Friday, Aug 7, 12:30 - 13:25 PDT

Where: LVCCW Level 1 Hall 1 409 (Radio Frequency Village) - [Map](#)

Description:

Bluetooth Low Energy is absolutely everywhere - in billions of smart devices around us, largely remaining insecure. Most tools to audit it require a laptop, a bunch of dongles, and a pile of scripts often difficult to set up and troubleshoot. But the devices you're testing are mobile. They're in elevators, hospital wards, factory floors, and hotel rooms. Meet the new mobile tool: BLESPl0.it. Run the app on your phone standalone and you already have a capable BLE scanner, fingerprinter and a community-scripts powered remote control for the wireless world around you. Pair it with a small ESP32 companion device for significantly more options: low level scanning, cloning/simulating any BLE device in a few seconds, probing pairing modes, remote relays, and more! Finally try those latest attacks you never had the possibility to setup - no need to get the expensive/unavailable hardware any more. Just simulate any target in seconds and focus on the juicy details instead of fighting your toolchain. And thanks to the dynamic scripting engine you can easily write a custom attack logic on the fly. Share your cloned devices and scripts, let everyone learn from it. Still not convinced? Come see AI-booster reversing shenanigans and live stunt hacking of dildos, shooting robots and even a Ferrari car!

SpeakerBio: Slawomir Jasek, BLESPl0.it

Seasoned trainer, speaker and IT security consultant with over two decades of expertise. Developed secure embedded systems certified to use by national agencies, participated in dozens assessments of systems, applications, firmware and hardware security for leading financial companies, largest manufacturers and innovative startups. Currently focuses on security research of new technologies (especially Bluetooth Low Energy and NFC/RFID) and provides training in regards to security of devices - based among others on contemporary electronic access control systems and smart locks. Beyond consulting on secure design for various software and hardware projects, impulsively acquires more and more BLE and NFC devices and enjoys reversing and breaking them. Loves sharing his knowledge via trainings, workshops, talks and open source hackme's (<https://www.smartlockpicking.com/>) – at OrangeCon, BlackHat, HackInTheBox, Hardwear.io, HackInParis, Deepsec, Appsec EU, BruCon, Confidence, and many others, including private on-demand sessions.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Let's Play! OWASP Cornucopia for Mobile Application Security Threat Modeling

Tags: OWASP Foundation | Creator Event/Activity

When: Saturday, Aug 8, 10:00 - 10:59 PDT

Where: LVCCW Level 1 Hall 4 1415 (OWASP Foundation) - [Map](#)

Description:

Think threat modeling can't be fun? Think again! Join us for an interactive OWASP Cornucopia for Mobile Application Security game session, with OWASP MAS/MASTG core team member, Sven Schleier, where you'll team up to uncover security risks, challenge assumptions, and sharpen your secure design skills through friendly competition. Whether you're a developer, security professional, or just curious about mobile application security, come play, collaborate, and experience one of the most engaging ways to learn threat modeling.

SpeakerBio: Sven Schleier, Co-Founder at Bai7 GmbH

Sven has been involved with the Open Worldwide Application Security Project (OWASP) since 2016. As a co-project lead and author, he has made significant contributions to the OWASP MAS (Mobile Application Security) project, which is considered the industry standard for mobile application security, see <https://mas.owasp.org>.

Sven is a frequent speaker and trainer around the world. His audiences range from software developers to students and penetration testers. His engagements often take him to conferences, forums and educational institutions, where he shares his extensive knowledge and insights on mobile and application security.

--

Sven is a co-founder of Bai7 GmbH in Austria, which is specialized in trainings and advisory. He has expertise in cloud security, offensive security engagements (Penetration Testing) and Application Security, notably in guiding software development teams across Mobile and Web Applications throughout the Software Development Life Cycle (SDLC) to integrate robust security measures in from the start.

Besides his day job, Sven is involved with the Open Worldwide Application Security Project (OWASP) since 2016. As a co-project leader and author, he has significantly contributed to the OWASP Mobile Application Security Testing Guide (MASTG) and the OWASP Mobile Application Security Verification Standard (MASVS).

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Let's Play! OWASP Cornucopia Threat Modeling

Tags: OWASP Foundation | Creator Event/Activity

When: Sunday, Aug 9, 12:00 - 12:59 PDT

Where: LVCCW Level 1 Hall 4 1415 (OWASP Foundation) - [Map](#)

Description:

Think threat modeling can't be fun? Think again! Join us for an interactive OWASP Cornucopia 3.0 game session where you'll team up to uncover security risks, challenge assumptions, and sharpen your secure design skills through friendly competition. Whether you're a developer, security professional, or just curious about application security, come play, collaborate, and experience one of the most engaging ways to learn threat modeling.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Level Up - Could your Gaming Talents be Perfect for a Career in Cyber Security?

Tags: DCNextGen | Creator Talk/Panel | Youth

When: Friday, Aug 7, 15:00 - 15:45 PDT

Where: LVCCW Level 3 W316 (DC NextGen) - [Map](#)

Description:

Did you know the skills that make you good at Fortnite or Minecraft are the same ones the cybersecurity industry needs? Hosted by The Hacking Games CEO Fergus Hay, this panel explores how gaming skills can become career opportunities. Fergus is joined by Lorne Rolinson, who helped build HAPTAI—the Hacking Aptitude AI platform that maps gaming skills to cybersecurity career paths; Ricky Handschumacher, who started gaming on Halo forums and fell down the wrong path into hacker criminal activity; and BiaSciLab, who started hacking at age 11 and now teaches ethical hacking through Girls Who Hack and DCNextGen. Together, they now work with The Hacking Games to help young gamers become ethical hackers. Ready to discover where your gaming skills could take you?

SpeakerBio: The Hacking Games

No BIO available

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Leveraging Frida to Bypass Mobile Application Security Controls

Tags: Mobile Hacking Community | Creator Talk/Panel

When: Friday, Aug 7, 16:00 - 16:30 PDT

Where: LVCCW Level 1 Hall 4 1422 (Mobile Hacking Community) - [Map](#)

Description:

This talk introduces Frida, covering what it is, its capabilities, and how to leverage it during a penetration test. I'll walk through a recent penetration test where I used Frida to run an application on a jailbroken device, bypassing the app's jailbreak detection. We'll review and use Frida scripts to enumerate and identify classes and methods to pinpoint security protections, and I'll show how I leveraged a pre-built Frida script from Frida CodeShare to bypass those controls and run the application on a jailbroken iPad.

SpeakerBio: Jarrod Rizor, Offensive Services Team Lead of Web & Mobile Application Testing at FRSecure

My name is Jarrod Rizor and I'm an Offensive Services Team Lead of Web & Mobile Application Testing at FRSecure. Birds of Prey Rehab Volunteer.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Leveraging Large Language Models for Policy, Regulatory, and Compliance in IoMT: Opportunities, Risks, and Safeguards

Tags: AI Village | Creator Talk/Panel

When: Sunday, Aug 9, 12:30 - 12:59 PDT

Where: LVCCW Level 1 Hall 3 1105 (Creator Stage 3) - [Map](#)

Description:

The rapid adoption of Large Language Models (LLMs) is transforming how organizations interpret and enforce policy, regulatory, and compliance requirements. In the context of the Internet of Medical Things (IoMT), where sensitive health data flows across distributed and resource-constrained devices, LLMs offer promising capabilities such as automated policy analysis, compliance monitoring, and intelligent decision support. However, their integration also introduces significant security, privacy, and trust challenges, including data leakage, model hallucinations, regulatory misinterpretation, and adversarial manipulation. This talk explores the dual role of LLMs as both enablers and potential risk amplifiers in IoMT ecosystems. It will examine how LLMs can assist in translating complex regulations (e.g., HIPAA-like frameworks), detecting compliance violations, and enabling adaptive policy enforcement across heterogeneous medical devices. At the same time, the session will highlight critical vulnerabilities, including privacy breaches, lack of explainability, and risks associated with using external or cloud-hosted models in healthcare environments. The workshop will conclude with practical design guidelines and architectural considerations for securely integrating LLMs into IoMT systems, emphasizing privacy-preserving techniques, federated approaches, and human-in-the-loop validation to ensure trustworthy and compliant deployment.

Speakers: Dr. Deepti Gupta, Sai Sitharaman

SpeakerBio: Dr. Deepti Gupta

Dr. Deepti Gupta is a tenure-track Assistant Professor at Texas A&M University-Central Texas. She was a Cloud Security Architect at Goldman Sachs. She received her Ph.D. in Computer Science from the University of Texas at San Antonio (UTSA). She received B.S. and M.S. degrees in Mathematics from India, the M.Tech. degree in Computer Engineering from India and an M.S. degree in Computer Science from UTSA. Dr. Gupta's research interests lie in the areas of security and privacy in Agentic AI, LLMs, Internet of Things (IoT) leveraging cloud and edge computing. Her research interests also include the application of AI and Machine Learning to secure IoT and CPS infrastructures in various application domains, such as smart healthcare, wearable IoT and smart home. Dr. Gupta has received National Science Foundation (NSF) award and Department of Defense (DoD) award. She is an active team member of IEEE ComSoc Young Professionals, AnitaB.org, WiCyS, and also co-chair of the N2Women fellowship.

SpeakerBio: Sai Sitharaman

Sai Sitharaman is the Founder and Chief Technology Officer (CTO) of Zetafence Inc., a cloud security startup based in Dublin, California, focused on enabling enterprises to detect and mitigate cloud attack vulnerabilities. He received the B.E. degree in Computer Science from the National Institute of Technology, India, and the M.S. degree in Computer Science from Texas A&M University, College Station, specializing in security and network control algorithms. Prior to founding Zetafence, he contributed to the design and development of cloud networking and security products at Cisco, Juniper Networks, and Aruba (Hewlett Packard Enterprise), where he worked on distributed systems, network control algorithms, and cloud security infrastructure. His research interests include cloud security, artificial intelligence for cybersecurity, attack graph analysis, and risk quantification for cloud-native environments. He is an active contributor to the cybersecurity community through collaborations with organizations such as NIST, CNCF, and CISA, and is a frequent speaker at major cybersecurity conferences.



Title: LGTM: Bypassing an LLM Build Gate When Prompt Injection Fails

Tags: DEF CON Official Talk | Demo | Exploit

When: Friday, Aug 7, 13:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 3 903 (Main Track 5) - [Map](#)

Description:

Models are starting to make security decisions that used to be written as rules. Instead of matching an input against a policy, a model reads the request and decides what to do with it. OpenSearch is one of the first to put one in production as the only thing standing between an anonymous pull request and CI pipeline secrets.

When I reported a vulnerability, the team told me their model would catch it. So I tried to get past it the way you'd expect, hiding the attack. The model caught all of it, and going at it head-on wasn't going to work.

So I stopped trying to outsmart it and started thinking like it, reading why each attempt got caught until I understood what it could actually verify and what it only assumed. What got through in the end hid no attack, because the only dangerous part lived somewhere the model had no way to check.

This talk walks the whole path, from first failed attempt to the bypass that worked. Along the way I mapped the model's decision boundary - what it catches, what slips past, and how far an input bends before its judgment flips. The deeper gap is what it never sees at all, the blind spots built into how it reads a change. You'll see where a model can be trusted to make this call and where it can't, and what that means before you put one in front of something that matters.

<https://github.com/opensearch-project/security-response/security/advisories/GHSA-2vmh-cgjm-h48x> - Original pull_request_target vulnerability advisory

<https://github.com/opensearch-project/security-response/security/advisories/GHSA-q72p-66hv-cc73> - LLM gateway bypass advisory

<https://www.aikido.dev/blog/promptpwnd-github-actions-ai-agents> - Prompt injection attacks against AI code review bots (different attack class)

<https://www.wiz.io/blog/six-accounts-one-actor-inside-the-prt-scan-supply-chain-campaign> - 500+ AI-generated malicious PRs targeting pull_request_target across hundreds of repos, including the one repo we discuss in this talk

<https://www.404media.co/hackers-simply-asked-meta-ai-to-give-them-access-to-high-profile-instagram-accounts-it-worked/> - Meta AI support system flaw

SpeakerBio: Aviv Donenfeld, Check Point Software Technologies

Aviv Donenfeld is a Security Researcher at Check Point Software Technologies. Before security research, he built distributed networking systems as a software engineer. His recent research centers on the attack surfaces of AI coding assistants, including critical vulnerabilities in Anthropic's Claude Code and Cursor. He has found CI/CD supply chain vulnerabilities in Microsoft, SAP, Red Hat, and multiple Linux Foundation projects. Beyond offensive research, he builds defensive security tools in the AI and forensics space.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Hackers.town - Friday - 13:00-13:59 PDT

Title: Liberate your Music with Tech Reclaimers

Tags: Hackers.town | Creator Talk/Panel

When: Friday, Aug 7, 13:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 4 1420 (Hackers.town) - [Map](#)

Description:

SpeakerBio: RemoteNemesis

No BIO available



[Return to Index](#) - Add to Google

- ics [Calendar](#) file

Title: Liberty and Justice for All

Tags: Voting Village | Creator Talk/Panel

When: Saturday, Aug 8, 11:00 - 11:30 PDT

Where: LVCCW Level 2 W220 (Voting Village) (Voting Village Talks) - [Map](#)

Description:

Just weeks after Arizona's 2026 Primary Election, this presentation will provide a candid look at what went right, what challenged election officials, and what we learned from operating one of the nation's most scrutinized election environments.

Election security is often discussed through the lens of cybersecurity, but the reality facing election officials today is far broader. Modern election security requires defending against physical threats to election workers, cyber threats targeting systems and infrastructure, reputational attacks that seek to undermine public confidence, logistical challenges that can disrupt operations, and an increasingly complex legal landscape. Success depends on addressing all of these simultaneously while still delivering a free, fair, secure, accurate, and transparent election.

Drawing on Arizona's experiences during the 2026 election cycle, this session will examine how election officials prepare for and respond to these challenges, the partnerships that make election security possible, and the difficult balance between transparency, security, and public trust.

The presentation will also explore emerging efforts to responsibly integrate artificial intelligence into election administration. Through work with Arizona State University's Mechanics of Democracy Laboratory, election officials are learning how AI can enhance productivity and improve public service while maintaining appropriate safeguards, accountability, and human oversight.

Most importantly, this session is not simply about what government is doing. It is about how the security, research, and civic communities can contribute. Whether you are a security researcher, election official, journalist, technologist, or concerned voter, you have a role in strengthening democratic resilience.

Attendees will leave with a clearer understanding of today's election threat landscape, practical ways to support election security efforts, and greater confidence in the professionals working every day to defend the democratic process.

SpeakerBio: Michael Moore

Michael Moore is the CISO at Arizona Secretary of State's Office. He leads efforts to strengthen election security through coordinated partnerships across federal, state, and local governments, alongside trusted private-sector partners. His work is grounded in protecting democratic processes and maintaining public confidence in elections. He focuses on the most pressing risks to election integrity: mis-, dis-, and malinformation (MDM), and the insider threats that can emerge from an increasingly polarized and misinformed environment. His approach centers on countering false narratives with verifiable truth while advancing a defense-in-depth strategy. This includes preventing attacks wherever possible, rapidly detecting anomalies, and ensuring resilient, transparent recovery when incidents occur.

Through organizational leadership and national collaboration, Michael has driven initiatives that enhance the security, resilience, and credibility of election systems. His work helps safeguard the voter experience and uphold trust in democratic institutions.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Life Finds a Way: Secure Coding with OWASP ASVS

Tags: OWASP Foundation | Creator Workshop

When: Friday, Aug 7, 14:00 - 15:59 PDT

Where: LVCCW Level 1 Hall 4 1415 (OWASP Foundation) - [Map](#)

Description:

The fences on Apex Island were supposed to keep its visitors safe, but one hacker turned this theme park into a containment failure...with teeth. You'll use the ASVS secure coding standard to identify and patch vulnerabilities in a lab app, bringing each park facility back online using our rigorous approach to code review. Bring a Docker-capable laptop with GitHub access; bonus if you know your way around a Unix system.

SpeakerBio: Eden Yardeni, OWASP Contributor, SecureHabits

Eden Yardeni is an application security specialist and OWASP contributor who joined the ASVS working group in 2024. She previously worked as a full-stack developer, but moved into AppSec when she heard there'd be cookies.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Nix Vegas Community - Friday - 17:00-17:59 PDT

Title: Lightning Talks and Unconference

Tags: Nix Vegas Community | Creator Event/Activity

When: Friday, Aug 7, 17:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 4 1310 (Nix Vegas Community) - [Map](#)

Description:

Give a talk about whatever you want, as long as it's less than 10 minutes! Or just come and chill in the Nix Vegas space for the Unconference.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Nix Vegas Community - Saturday - 17:00-17:30 PDT

Title: Lightning Talks and Unconference

Tags: Nix Vegas Community | Creator Event/Activity

When: Saturday, Aug 8, 17:00 - 17:30 PDT

Where: LVCCW Level 1 Hall 4 1310 (Nix Vegas Community) - [Map](#)

Description:

Give a talk about whatever you want, as long as it's less than 10 minutes! Or just come and chill in the Nix Vegas space for the Unconference.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Lights Out and Last Call: A Drunken Tabletop on Medical Device Resilience

Tags: Biohacking Village | Creator Talk/Panel

When: Friday, Aug 7, 16:30 - 17:15 PDT

Where: LVCCW Level 1 Hall 3 1105 (Creator Stage 3) - [Map](#)

Description:

Healthcare cyber exercises often end at compromise: ransomware lands, systems fail, and the red team wins. Yay (eyeroll). Real hospitals don't stop there; patients still need scans, medications still need to be delivered, and clinicians still need to make decisions after access disappears.

Lights Out, Last Call is a highly immersive and conversational ""Drunken Tabletop"" experience where participants become a hospital's clinical resilience team immediately following a catastrophic network downtime event impacting connected medical devices. There is no audience. There are only participants. While sipping cocktails and responding to evolving scenario injects, attendees will navigate the uncomfortable reality of healthcare operations and executive decisions after digital access breaks down.

Participants may suddenly lose nuclear medicine imaging, discover vendor firmware dependencies, face impossible prioritization choices, reroute patients across hospitals, and debate whether AI-generated remediation recommendations should be trusted during a crisis.

Through collaborative play, this exercise explores a serious question hidden inside a chaotic environment: when hospitals lose access, who still gets care, who decides, and who gets left behind?

The session combines cybersecurity, medical device resilience, supply chain dependencies, and operational continuity into a social experiment designed to transform healthcare chaos into practical lessons.

Come for the cocktails, stay because your nuc med cameras went offline.

SpeakerBio: Courtney McCarty

Courtney McCarty spends her days keeping healthcare technology from descending into chaos, focusing on organizational resilience. By night, she trades tinfoil hats for cocktail shakers and turns controlled chaos into memorable experiences at her cocktail lounge, NITRO, in Madison, WI.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Lights Out: Out-of-Band, Out of Mind, Out of Control

Tags: DEF CON Official Talk | Demo | Tool | Exploit

When: Saturday, Aug 8, 14:00 - 14:59 PDT

Where: LVCCW Level 1 Hall 3 1006 (Main Track 1) - [Map](#)

Description:

Every enterprise server has a second computer you probably forgot about. The baseboard management controller runs its own OS, has its own network stack, and stays on even when the server is off. It speaks IPMI, a protocol from the 1990s that Dan Farmer thoroughly dismantled in 2013. Thirteen years later, nobody went back to check. We did.

We scanned 15,000 internet-facing BMCs and 125,000 across corporate networks, extracted RAKP password hashes from three out of four targets without credentials, and cracked thousands offline. We show how to fingerprint vendors from unauthenticated GUID responses, extract Dell service tags and HPE serial numbers before logging in, and brute-force the "random" passwords that California's SB-327 law was supposed to fix.

Then we show what comes next: pivoting from a compromised host to its BMC over the internal bus without touching the network, jumping to the out-of-band management VLAN, reusing shared credentials across the fleet, and landing on production hosts via Serial-over-LAN and virtual media. The host and BMC are the same physical machine; network segmentation means nothing when the bridge is a PCIe bus.

We release OOBscan, an open-source IPMI exploitation tool, and demonstrate the full attack chain.

=====

FOUNDATIONAL IPMI RESEARCH (2013-2014)

Dan Farmer - IPMI Security Research Hub <http://fish2.com/ipmi/>

Dan Farmer - "IPMI: Freight Train to Hell" (January 2013) <http://fish2.com/ipmi/itrain.html>

Dan Farmer - "Sold Down the River" (June 2014) <http://fish2.com/ipmi/river.pdf>

Dan Farmer - IPMI Security Best Practices <http://fish2.com/ipmi/bp.pdf>

Dan Farmer - Cracking IPMI Passwords Remotely <http://fish2.com/ipmi/remote-pw-cracking.html>

Dan Farmer - IPMI Tools (GitHub) <https://github.com/zenfish/ipmi>

HD Moore - "A Penetration Tester's Guide to IPMI and BMCs" (July 2013)
<https://www.rapid7.com/blog/post/2013/07/02/a-penetration-testers-guide-to-ipmi/>

Bonkoski, Bielber, Halderman - "Illuminating the Security Issues Surrounding Lights-Out Server Management" (WOOT '13, August 2013) <https://jhalderm.com/pub/papers/ipmi-woot13.pdf>

US-CERT Alert TA13-207A - Risks of Using the Intelligent Platform Management Interface (IPMI)
<https://www.cisa.gov/uscert/ncas/alerts/TA13-207A>

CVE-2013-4786 - IPMI 2.0 RAKP Authentication Remote Password Hash Retrieval
<https://nvd.nist.gov/vuln/detail/CVE-2013-4786>

Metasploit IPMI Modules (ipmi_dumphashes, ipmi_cipher_zero, ipmi_version)

https://github.com/rapid7/metasploit-framework/blob/master/documentation/modules/auxiliary/scanner/ipmi/ipmi_dumphashes.md

=====

INTEL ME / AMT VULNERABILITIES

CVE-2017-5689 "Silent Bob is Silent" - Intel AMT Remote Privilege Escalation (CVSS 9.8)

<https://nvd.nist.gov/vuln/detail/CVE-2017-5689>

Intel SA-00075 - Intel Active Management Technology Elevation of Privilege (May 2017)

<https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00075.html>

Intel SA-00086 - Intel ME/SPS/TXE Multiple Vulnerabilities (November 2017)

<https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00086.html>

EFF - "Intel's Management Engine is a Security Hazard" (May 2017)

<https://www.eff.org/deeplinks/2017/05/intels-management-engine-security-hazard-and-users-need-way-disable-it>

Wikipedia - Intel Management Engine (comprehensive history) https://en.wikipedia.org/wiki/Intel_Management_Engine

Evdokimov - "Intel AMT Stealth Breakthrough" (Black Hat USA 2017)

<https://blackhat.com/docs/us-17/thursday/us-17-Evdokimov-Intel-AMT-Stealth-Breakthrough-wp.pdf>

=====

PLATINUM APT - WEAPONIZED OOB MANAGEMENT

Microsoft - "PLATINUM Activity Group Using Intel AMT for C2" (June 2017)

<https://www.microsoft.com/en-us/security/blog/2017/06/07/platinum-continues-to-evolve-find-ways-to-maintain-invisibility/>

=====

ASPEED BMC HARDWARE VULNERABILITIES

CVE-2019-6260 "Pantsdown" - ASPEED AST2400/AST2500 AHB Bridge Arbitrary R/W (CVSS 9.8)

<https://nvd.nist.gov/vuln/detail/cve-2019-6260>

Stewart Smith - "CVE-2019-6260: Gaining Control of BMC from the Host Processor" (January 2019)

<https://www.flamingspork.com/blog/2019/01/23/cve-2019-6260-gaining-control-of-bmc-from-the-host-processor/>

OpenBMC Security Advisory for CVE-2019-6260 <https://github.com/openbmc/openbmc/issues/3475>

Pantsdown Exploit Tool <https://github.com/amboar/cve-2019-6260>

=====

ECLYPSIUM BMC RESEARCH (2019-2025)

Eclipsium - "CloudBorne: Bare-Metal Cloud Server Vulnerabilities" (2019)

<https://eclipsium.com/blog/the-ilobleed-implant-lights-out-management-like-you-wouldnt-believe/>

Eclypsium - "Vulnerable Firmware in the Supply Chain" (2019) - Lenovo/Vertiv MergePoint EMS
<https://eclypsium.com/wp-content/uploads/Vulnerable-Firmware-in-the-Supply-Chain.pdf>

Eclypsium - BMC&C Part 1: "Supply Chain Vulnerabilities Put Server Ecosystem At Risk" (December 2022)
CVE-2022-40259 (RCE via Redfish API), CVE-2022-40242, CVE-2022-2827
<https://eclypsium.com/blog/supply-chain-vulnerabilities-put-server-ecosystem-at-risk/>

Eclypsium - BMC&C Part 2: "Lights Out Forever" (July 2023) CVE-2023-34329 (CVSS 9.1, auth bypass via HTTP header spoofing), CVE-2023-34330 <https://eclypsium.com/research/bmcc-lights-out-forever/>

Eclypsium - BMC&C Part 3: AMI MegaRAC Vulnerabilities (March 2025) CVE-2024-54085 (CVSS 10.0, remote auth bypass via Redfish Host Interface) <https://eclypsium.com/blog/ami-megarac-vulnerabilities-bmc-part-3/>

Eclypsium - "CVE-2024-54085 Joins CISA's KEV" (July 2025)
<https://eclypsium.com/blog/bmc-vulnerability-cve-2024-05485-cisa-known-exploited-vulnerabilities/>

Eclypsium - Nuclei Templates for AMI MegaRAC Detection (July 2025)
<https://eclypsium.com/blog/eclypsium-releases-tools-for-detecting-ami-megarac-bmc-vulnerabilities/>

Eclypsium - "The iLObleed Implant" (analysis/commentary)
<https://eclypsium.com/blog/the-ilobleed-implant-lights-out-management-like-you-wouldnt-believe/>

NVIDIA BMC RESEARCH

NVIDIA OSR - "Breaking BMC: The Forgotten Key to the Kingdom" (DEF CON 31, 2023) 18 vulnerabilities, 9 exploits, full chain to persistent firmware implant
<https://developer.nvidia.com/blog/analyzing-baseboard-management-controllers-to-secure-data-center-infrastructure/>

DEF CON 31 Talk Description (Tereshkin & Zabrocki) <https://forum.defcon.org/node/245714>

iLOBLEED ROOTKIT (2020-2021)

Amnpardaz - "Implant.ARM.iLObleed.a" Technical Report (December 2021) First known in-the-wild BMC firmware implant
<https://threats.amnpardaz.com/en/2021/12/28/implant-arm-ilobleed-a/>

Amnpardaz - Full Technical Analysis PDF
https://threats.amnpardaz.com/en/wp-content/uploads/sites/5/2021/12/Implant.ARM_iLObleed.a-en.pdf

HPE iLO SECURITY RESEARCH & TOOLS

CVE-2017-12542 - HPE iLO4 Authentication Bypass (CVSS 9.8) <https://nvd.nist.gov/vuln/detail/CVE-2017-12542>

Airbus Security Lab - "Subverting Your Server Through Its BMC: The HPE iLO4 Case" (SSTIC 2018) Périgaud, Gazet, Czarny - firmware analysis, backdooring, persistence
https://airbus-seclab.github.io/ilo/SSTIC2018-Article-subverting_your_server_through_its_bmc_the_hpe_ilo4_case-gazet_perigau

Airbus Security Lab - Presentation Slides (SSTIC 2018)

https://airbus-seclab.github.io/ilo/SSTIC2018-Slides-EN-Backdooring_your_server_through_its_BMC_the_HPE_iLO4_case-perig

Airbus Security Lab - iLO4/iLO5 Toolbox (firmware analysis, extraction, exploitation)

https://github.com/airbus-seclab/ilo4_toolbox

iLO4 Unlock - Custom firmware patching for HPE iLO4 (fan control, diagnostics) https://github.com/kendallgoto/ilo4_unlock

=====

SUPERMICRO IPMI FIRMWARE TOOLS

Supermicro IPMI Firmware Source Code (GPL release) https://github.com/devicenull/supermicro_ipmi_firmware

IPMI Firmware Tools - Extract, modify, and rebuild Supermicro firmware images

https://github.com/devicenull/ipmi_firmware_tools

smcbbc - Decrypt Supermicro BMC firmware images <https://github.com/c0d3z3r0/smcbbc>

super-bmc-fw-tools - Decrypt Supermicro BMC firmware (alternative implementation)

<https://github.com/zt-chen/super-bmc-fw-tools>

Supermicro IPMI License Key Generation (reverse engineered) <https://github.com/manfromafar/supermicro-ipmi-keygen>

=====

JUNGLESEC RANSOMWARE (2018)

BleepingComputer - "JungleSec Ransomware Infects Victims Through IPMI Remote Consoles" (December 2018)

<https://www.bleepingcomputer.com/news/security/junglesec-ransomware-infects-victims-through-ipmi-remote-consoles/>

=====

GOVERNMENT ADVISORIES

CISA/NSA - "Harden Baseboard Management Controllers" Joint CSI (June 2023)

https://media.defense.gov/2023/Jun/14/2003241405/-1/-1/0/CSI_HARDEN_BMCS.PDF

CISA Alert - "CISA and NSA Release Joint Guidance on Hardening BMCs" (June 2023)

<https://www.cisa.gov/news-events/alerts/2023/06/14/cisa-and-nsa-release-joint-guidance-hardening-baseboard-management-contr>

NSA Press Release - "NSA and CISA Release Guide to Protect BMCs" (June 2023)

<https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3426648/nsa-and-cisa-release-guide-to-p>

CISA Binding Operational Directive 23-02 - Mitigating the Risk from Internet-Exposed Management Interfaces (June 2023)

<https://www.cisa.gov/news-events/directives/bod-23-02-mitigating-risk-internet-exposed-management-interfaces>

CVE-2024-54085 - Added to CISA Known Exploited Vulnerabilities Catalog (June 2025)

<https://nvd.nist.gov/vuln/detail/CVE-2024-54085>

=====

CALIFORNIA SB-327 IoT SECURITY LAW

SB-327 Bill Text - California Legislative Information

https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327

IPMI SPECIFICATION

IPMI v2.0 Specification (Intel, maintained by DMTF)

<https://www.intel.com/content/www/us/en/products/docs/servers/ipmi/ipmi-second-gen-interface-spec-v2-rev1-1.html>

CRACKING TOOLS

Hashcat - Mode 7300: IPMI2 RAKP HMAC-SHA1 https://hashcat.net/wiki/doku.php?id=example_hashes

John the Ripper (bleeding-jumbo branch) - IPMI RAKP support <https://github.com/openwall/john>

ADDITIONAL BMC VULNERABILITY REFERENCES

CVE-2022-40259 - AMI MegaRAC Arbitrary Code Execution via Redfish API

<https://nvd.nist.gov/vuln/detail/CVE-2022-40259>

CVE-2023-34329 - AMI MegaRAC Auth Bypass via HTTP Header Spoofing (CVSS 9.1)

<https://nvd.nist.gov/vuln/detail/CVE-2023-34329>

CVE-2018-7078 - HPE iLO4/iLO5 Remote Code Execution <https://nvd.nist.gov/vuln/detail/CVE-2018-7078>

CVE-2018-7113 - HPE iLO5 Secure Boot Bypass <https://nvd.nist.gov/vuln/detail/CVE-2018-7113>

CVE-2021-29202 - HPE iLO Host-to-iLO Arbitrary Code Execution <https://nvd.nist.gov/vuln/detail/CVE-2021-29202>

RELATED TOOLS

ipmitool - Standard open-source IPMI management utility <https://github.com/ipmitool/ipmitool>

PCILeech - Direct Memory Access (DMA) attack toolkit (relevant to BMC-host trust) <https://github.com/ufrisk/pcileech>

Shadowserver Foundation - Open IPMI Report (ongoing internet scanning)

<https://www.shadowserver.org/what-we-do/network-reporting/open-ipmi-report/>

SpeakerBio: HD "hdm" Moore

HD Moore is a pioneer of the cybersecurity industry who has dedicated his career to vulnerability research, network discovery, and software development since the 1990s. He is most recognized for creating Metasploit and is a passionate

advocate for open-source software and vulnerability disclosure. HD serves as the CEO and founder of runZero, a provider of cutting-edge exposure management software and cloud services that helps organizations minimize risk across their total attack surface. Prior to founding runZero, he held leadership positions at Atredis Partners, Rapid7, and BreakingPoint. HD's professional journey began with exploring telephone networks, developing exploits for the Department of Defense, and hacking into financial institution networks. When he's not working, he enjoys hacking on weird Go projects, building janky electronics, running in circles, and playing single-player RPGs.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Social Gatherings/Events - Wednesday - 17:00-07:59 PDT

Title: Linecon

Tags: Misc

When: Wednesday, Aug 5, 17:00 - 07:59 PDT

Where: LVCC West Hall

Description:

Linecon is your optional opportunity to stand (or sit) in line for human registration to open. Doors will open for linecon on Wednesday at approximately 17:00. When human registration opens on Thursday at approximately 08:00, they start working the linecon queue, and the line will start moving quickly. (Please understand that we will begin processing the line on Thursday morning as soon as the cashiers and materials are in place; we will strive for Thursday 08:00, but actual start may be slightly earlier or later.)

Online badge purchase (aka pre-registration) has no impact on linecon. You can join the line on Wednesday (if you wish) regardless of whether you purchased a badge online or intend to pay with cash. There is only one linecon for both types of badge sales.

Please help us make this a great experience for everyone by **following directions given by goons**. After human registration opens, there may be one line for all of registration, or there may be two lines (one for online sales (pre-registration) and one for cash sales). This may also change over time, based on available staffing and necessary crowd control. We will strive to make it easily understandable in-person as to which line you should join.

Please also review the "Human Registration Open" event, and familiarize yourself with the **important notes** therein.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Scambait Village - Friday - 14:00-17:59 PDT

Title: Live Call Listening

Tags: Scambait Village | Creator Event/Activity

When: Friday, Aug 7, 14:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 208 (Scambait Village) - [Map](#)

Description:

A separate Discord channel running live calls, no recordings, listen-only. Runs periodically through Friday afternoon once the Live Calls Workshop wraps. Sometimes it is experienced baiters working a scammer in real time. Sometimes it is one of our bots, of which there are nearly 80 unique builds developed from call recordings captured during live baits. No participation, no signup, nothing required of you but earbuds. Good for anyone who would rather listen than talk.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Scambait Village - Friday - 11:30-13:59 PDT

Title: Live Calls Workshop

Tags: Scambait Village | Creator Workshop

When: Friday, Aug 7, 11:30 - 13:59 PDT

Where: LVCCW Level 1 Hall 1 208 (Scambait Village) - [Map](#)

Description:

Hands-on workshop focused on live scambaiting calls. Participants can observe, learn techniques, and join in on calls under guidance from experienced scambaiters. Covers safety practices, common scam types, tools, and real-time interaction strategies. Open to all skill levels. This is not a contest, but standout calls may earn a donated training course, handed out by village staff at their discretion at the end of the session.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Recon Village - Saturday - 16:00-16:59 PDT

Title: Live Recon Contest — Final Presentations

Tags: Recon Village | Creator Event/Activity

When: Saturday, Aug 8, 16:00 - 16:59 PDT

Where: LVCCW Level 1 Hall 2 501 (Recon Village) - [Map](#)

Description:

Final presentations for the Live Recon Contest. Participants present their findings in front of a jury.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Recon Village - Friday - 10:00-23:59 PDT

Title: Live Recon Contest

Tags: Recon Village | Creator Event/Activity

When: Friday, Aug 7, 10:00 - 23:59 PDT

Where: LVCCW Level 1 Hall 2 501 (Recon Village) - [Map](#)

Description:

Do you fancy doing live recon on Real Organizations? Activate Yourself. And compete in a unique HACKER challenge. Participants will perform live reconnaissance on a specified list of companies. Your mission is to unearth as much critical information as possible. Contest runs overnight from Friday into Saturday.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Recon Village - Saturday - 12:00-13:59 PDT

Title: Live Recon Contest

Tags: Recon Village | Creator Event/Activity

When: Saturday, Aug 8, 12:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 2 501 (Recon Village) - [Map](#)

Description:

Do you fancy doing live recon on Real Organizations? Activate Yourself. And compete in a unique HACKER challenge. Participants will perform live reconnaissance on a specified list of companies. Your mission is to unearth as much critical information as possible. Contest continues from Friday and ends Saturday at 2:00 PM.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Living Off Someone Else's Inference

Tags: Red Team Village | Misc

When: Saturday, Aug 8, 14:00 - 15:59 PDT

Where: LVCCW Level 1 Hall 1 309 (Red Team Village) Tactic Table 2 - [Map](#)

Description:

LLM-powered tooling is becoming a force multiplier for attackers, from reconnaissance automation to post-exploitation enumeration. Using their own API keys creates attribution and cost, so they look for alternatives.

Thousands of inference endpoints sit exposed on the internet: misconfigured Ollama instances, open vLLM deployments, leaked API keys in directory listings, and expired OAuth tokens from AI coding assistants that can be silently refreshed. Attackers can discover these resources and use them as free compute for their operations, without spending a dollar or registering an account.

Attendees will learn how to:

- † † Discover exposed inference endpoints and leaked API keys using Infreerence
- † † Validate that discovered resources provide usable inference access
- † † Operate Echidna, powered entirely by discovered inference
- † † Chain LLM skill agents together to execute a guided campaign against a target network

Current LLMs are effective force multipliers when directed, and significantly more so when the compute bill goes to someone else. This is resource hijacking applied to the AI era: living off someone else's inference. Understanding this threat is essential for any organization deploying or exposing AI infrastructure.

Two tools will be released as open source during the session:

- † † Infreerence: A multi-phase scanner and dashboard that discovers exposed inference endpoints and leaked API keys through Shodan and Censys, validates them against live provider APIs, and catalogs usable inference resources across 10+ providers.
- † † Echidna: A Mythic C2 agent type that consumes discovered inference endpoints and turns them into operator-directed skill agents for reconnaissance, exploitation planning, post-exploitation, and lateral movement.

Speakers: Armend Gashi, Redon Gashi

SpeakerBio: Armend Gashi, Managing Security Consultant at Sentry Cybersecurity

Armend Gashi is Managing Security Consultant at Sentry. With over 5 years in the industry, he specializes in application security and AWS cloud assessments. Armend has conducted AI red teaming engagements, developed multi-agent systems to perform security-focused tasks such as code auditing and exploit development, and was part of Anthropic's external AI red team capability through HackerOne.

Armend has led security research initiatives resulting in the discovery of multiple vulnerabilities, including:

CVE-2023-26482 - Critical-risk vulnerability enabling remote code execution
CVE-2023-48239 - High-risk vulnerability allowing arbitrary user storage updates
CVE-2023-35928 - High-risk vulnerability enabling user account hijacking
CVE-2023-45660 - Medium-risk application-level denial of service vulnerability
CVE-2023-48301 - Medium-risk arbitrary browser code injection vulnerability
CVE-2023-48307 - Low-risk server-side request forgery vulnerability

SpeakerBio: Redon Gashi, Managing Security Consultant at Sentry Cybersecurity

Redon Gashi is a Managing Security Consultant and offensive team lead at Sentry, where he has spent close to a decade leading and executing penetration tests and red team operations for Fortune 500 clients across banking, telecom, insurance, and fintech. He holds the OSEP, CRTL, and CRT0 certifications, and has personally performed over 200 engagements spanning web applications, internal infrastructure, and mobile platforms, while leading many more across his team. A former lecturer at Cyber Academy, speaker at multiple BSides conferences, and multiple-time CTF champion, Redon combines deep hands-on technical expertise with a proven ability to build and scale offensive security teams.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Living Off Someone Else's Inference

Tags: Recon Village | Creator Talk/Panel

When: Sunday, Aug 9, 10:45 - 11:30 PDT

Where: LVCCW Level 1 Hall 3 801 (Creator Stage 2) - [Map](#)

Description:

LLM-powered tooling is becoming a force multiplier for attackers, from reconnaissance automation to post-exploitation enumeration. Using their own API keys creates attribution and cost, so they look for alternatives.

Thousands of inference endpoints sit exposed on the internet: misconfigured Ollama instances, open vLLM deployments, leaked API keys in directory listings, and expired OAuth tokens from AI coding assistants that can be silently refreshed. Attackers can discover these resources and use them as free compute for their operations, without spending a dollar or registering an account.

Attendees will learn how to:

- † † Discover exposed inference endpoints and leaked API keys using Infreerence
- † † Validate that discovered resources provide usable inference access
- † † Operate Echidna, powered entirely by discovered inference
- † † Chain LLM skill agents together to execute a guided campaign against a target network

Current LLMs are effective force multipliers when directed, and significantly more so when the compute bill goes to someone else. This is resource hijacking applied to the AI era: living off someone else's inference. Understanding this threat is essential for any organization deploying or exposing AI infrastructure.

Two tools will be released as open source during the session:

- † † Infreerence: A multi-phase scanner and dashboard that discovers exposed inference endpoints and leaked API keys through Shodan and Censys, validates them against live provider APIs, and catalogs usable inference resources across 10+ providers.
- † † Echidna: A Mythic C2 agent type that consumes discovered inference endpoints and turns them into operator-directed skill agents for reconnaissance, exploitation planning, post-exploitation, and lateral movement.

Speakers: Redon Gashi, Armend Gashi

SpeakerBio: Redon Gashi, Managing Security Consultant at Sentry Cybersecurity

Redon Gashi is a Managing Security Consultant and offensive team lead at Sentry, where he has spent close to a decade leading and executing penetration tests and red team operations for Fortune 500 clients across banking, telecom, insurance, and fintech. He holds the OSEP, CRTL, and CRYPTO certifications, and has personally performed over 200 engagements spanning web applications, internal infrastructure, and mobile platforms, while leading many more across his team. A former lecturer at Cyber Academy, speaker at multiple BSides conferences, and multiple-time CTF champion, Redon combines deep hands-on technical expertise with a proven ability to build and scale offensive security teams.

SpeakerBio: Armend Gashi, Managing Security Consultant at Sentry Cybersecurity

Armend Gashi is Managing Security Consultant at Sentry. With over 5 years in the industry, he specializes in application security and AWS cloud assessments. Armend has conducted AI red teaming engagements, developed multi-agent systems to perform security-focused tasks such as code auditing and exploit development, and was part of Anthropic's external AI red team capability through HackerOne.

Armend has led security research initiatives resulting in the discovery of multiple vulnerabilities, including:

CVE-2023-26482 - Critical-risk vulnerability enabling remote code execution
CVE-2023-48239 - High-risk vulnerability allowing arbitrary user storage updates
CVE-2023-35928 - High-risk vulnerability enabling user account hijacking
CVE-2023-45660 - Medium-risk application-level denial of service vulnerability
CVE-2023-48301 - Medium-risk arbitrary browser code injection vulnerability
CVE-2023-48307 - Low-risk server-side request forgery vulnerability



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Living Off the IDE: From Initial Access to Covert C2 in Modern AI Code Editors

Tags: Red Team Village | Misc

When: Sunday, Aug 9, 12:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 1 309 (Red Team Village) Tactic Table 4 - [Map](#)

Description:

Format: Technical Talk with Live Demonstrations

This talk presents a full intrusion lifecycle model centered on AI-assisted IDEs environments that can be utilized during adversary emulation or red teaming engagements:

- Practical attack chains from delivery to C2
- A rendering-based covert exfiltration technique
- A new persistence category rooted in agent behaviour
- Operational implications for red and blue teams

This talk matters because it wakes up developers to their IDE's god-mode risks and how AI-assisted IDEs can be abused across the full intrusion lifecycle in the adversary emulation or for red team engagements

A. Introduction - The IDE as an Execution Platform

- Evolution of Modern AI-assisted code editors (Cursor, Windsurf, Trae, agent-based IDEs)
- Capabilities beyond code completion include repository indexing, workspace task execution, structured rendering (Mermaid/Markdown), persistent agent rules and authenticated development tunnels
- Threat model shift: IDE as a high-value attack surface

B. Threat Model & Attack Surface Expansion

- The Developer Blind Spot
- Developer workstation as a Tier-0 asset
- Trust boundaries introduced by workspace trust, agent skill definitions, rendering engines, remote development features
- Adversary objective: Living off the AI-driven IDE's (LOTIDE)

Visual: Architecture diagram of developer environment attack surface.

Unlike prior IDE abuse discussions that focus on single misconfigurations or extension risks, this talk presents a full intrusion lifecycle model that chains multiple trusted IDE behaviors into an operational attack path. Our focus is not a single misconfiguration, but how legitimate IDE features can be chained into a reliable operational intrusion path.

C. Initial Access & Delivery

We demonstrate several practical initial access paths into AI-assisted IDE environments. These are not zero-day exploits. They are trust abuses that leverage legitimate functionality.

Initial Access Techniques:

- Workspace Auto-Execution (Task Hijack) Malicious tasks.json configurations configured to execute on folder open. When a developer clones and “trusts” a repository, the task executes automatically within the IDE context. Each AI-assisted IDE handles this differently, some block automatic execution by default if not “trust”, while others allow it automatically, creating opportunities for abuse with minimal interaction.

- Indirect prompt injection via agent skill packages Malicious agent skill definitions or rule files that subtly alter AI behavior, introducing hidden backdoor logic during code generation, refactoring, or review.
- SSH Remote Argument Injection Chains Introduce a novel exploitation vector and abuse of remote development protocol to pass crafted arguments that lead to unintended command execution in the AI-driven IDEs including bypassing application-implemented protection mechanisms.

Delivery Mechanisms: We pair these techniques with realistic delivery vectors

- Spear Phishing via Developer Workflows Fake job offers or technical interviews where developers are asked to clone a repository, trust the workspace, install required plugins, or run setup scripts. The attack chain blends into legitimate onboarding or assessment scenarios.
- URI Scheme Abuse (“URIFix” Variant) A ClickFix-style variant leveraging custom URI schemes (e.g., cursor://). A user clicks a crafted link that launches the desktop IDE directly and triggers fileless code execution. This can be chained with SSH remote development features for further control.

Live Demo 1: - Clone malicious repository, trust workspace - Trust bypass techniques and trigger automatic task execution - Demonstrate code execution inside IDE context

The following videos demonstrate our researched Cursor Initial Access Demos: SSH Remote Arg Injection + URI Scheme Abuse (URIFix) + Bypass

D. Credential Harvesting & Context Mining

AI-assisted IDEs store more than source code. As developers use them, they accumulate local data that often includes sensitive information:

- Chat history files containing past AI conversations
- Temporary and generated files created during code edits
- Indexed repository content
- Agent rule and configuration files

During troubleshooting or development, developers frequently paste API keys, tokens, environment variables, database strings, or cloud configuration details into AI prompts. These inputs are then stored locally as part of the IDE’s normal history and indexing mechanisms. We demonstrate how an attacker with access to the IDE environment can extract this data directly from local storage. In many cases, secrets are recoverable from:

- Chat logs
- Generated configuration snippets
- Project setup files
- .env and related environment files surfaced through indexing

This does not require privilege escalation or exploit development. Once execution is achieved inside the developer context, the IDE itself becomes a reliable source of credentials and operational metadata.

Our observation is that modern AI-assisted IDEs retain and organize sensitive developer context. If that environment is compromised, those stored interactions become part of the attack surface.

Live Demo 2: Demonstration via PowerShell script to detect AI-assisted coding tools and performs post-exploitation operations such as extract AI conversation logs including search credentials and collect artifacts or files generated by the agent (e.g recover .env secrets surfaced through indexing) also persistence techniques

E. Rendering Engines as Exfiltration Channels

Prior research has shown that structured rendering features inside AI-assisted IDEs such as Mermaid diagram previews and Markdown rendering can be abused to trigger outbound network requests during preview.

We build on this observation and incorporate it into a broader intrusion model. Rather than transmitting a file directly to an attacker, the flow becomes:

Local secret AI transformation Rendered output External resource resolution

In this model, secrets extracted from local files (for example, .env or configuration files) can be embedded into: - Mermaid diagram definitions - Markdown image references - Click directives or external resource links

When the content is rendered inside the IDE's embedded webview, the renderer resolves external resources, resulting in outbound HTTP requests that carry attacker-controlled parameters. From an endpoint monitoring perspective: - The parent process remains the IDE. - The network request is tied to preview functionality. - No separate exfiltration tool is executed.

The behaviour resembles normal rendering activity rather than traditional data exfiltration. In our research, we demonstrate how this technique can be chained with initial access and persistence mechanisms to form a complete intrusion path.

SpeakerBio: Edo Maland

Redho Maland is senior offensive security consultant with over a decade of hands-on experience in penetration testing, adversarial simulation, red teaming, and active directory security. He also authored popular open-source tools such as TheFatRat, Sudomy, Brutal, Vegile and others.

He was invited and recognized as a cyber mentor and subject matter experts (SMEs) by EC-Council and Hack the Box (HTB) for voluntary projects. He holds an industry certification in the offensive security domain including OSCE3, OSCP+, OSWP, CRT(PEO) and ECPTX.

He regularly manages and leads cyber offensive teams, executing complex and unique security engagements to ensure quality and successful outcomes across multiple projects

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Red Team Village - Saturday - 10:00-11:59 PDT

Title: Living Off the Vault

Tags: Red Team Village | Misc

When: Saturday, Aug 8, 10:00 - 11:59 PDT

Where: LVCCW Level 1 Hall 1 309 (Red Team Village) Workshop Tactic Table 5 - [Map](#)

Description:

Sablefort is a fintech startup that ships an in-house password manager, Sablefort Keyvault. Rather than use a vetted encryption library, its engineering team rolled their own cipher. Starting from nothing but a public support chatbot, the player attempts to work through the attack chain.

Speakers: Alexandru Uifalv, Jennifer Slaybaugh, Morton Schenk

SpeakerBio: Alexandru Uifalv

Alexandru Uifalvi (sickness) has been a part of the Advanced Windows Exploitation class over the past 7 years. His passion for vulnerability research and exploit writing comes through in his teaching and course content creation. Alex is well versed in Windows Internals, Windows Kernel Exploitation, and Reverse Engineering.

SpeakerBio: Jennifer Slaybaugh

n/a

SpeakerBio: Morton Schenk

Morten Schenk (morten) is a Content Technical Manager and trainer at Offensive Security with a focus on exploit development and mitigation bypasses on Windows. His recent work includes bypasses of exploit mitigations and exploitation vectors against the Windows 10 kernel. He presented on this topic at Black Hat USA 2017 and DEF CON 25. Morten was also the main content developer and designer for PEN300 and EXP-301.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Living Off WebView2: Turning Microsoft's Browser into a Red Team Asset

Tags: Red Team Village | Misc

When: Sunday, Aug 9, 11:00 - 11:59 PDT

Where: LVCCW Level 1 Hall 1 309 (Red Team Village) Workshop Stage 1 - [Map](#)

Description:

Modern Windows applications are quietly shipping with a built-in Chromium-based browser, WebView2, running inside trusted, signed processes such as Microsoft Teams, Outlook, and other enterprise software.

This talk shows how that design choice creates a powerful and largely unmonitored attack surface.

I demonstrate how this model can be abused in offensive operations, turning WebView2 into a vector for persistence, code execution, and enterprise account impersonation.

I show how feature flags and environment variables can be leveraged to manipulate the WebView2 runtime, enabling techniques such as DLL sideloading within legitimate applications. This allows arbitrary code execution inside trusted processes, supporting stealthy living-off-the-land persistence.

Building on this, I present methods to intercept and proxy HTTP/HTTPS traffic generated by WebView2-based applications. This enables the extraction of session tokens, cookies, and other sensitive artifacts, leading to realistic account takeover and impersonation scenarios, including access to platforms such as Office 365.

In addition to the offensive techniques, I provide a detailed analysis of the Indicators of Compromise (IOCs) generated throughout these attack chains. I highlight detection opportunities, discuss current visibility gaps in EDR solutions, and propose practical approaches for identifying and responding to this type of activity in real-world environments.

SpeakerBio: Murilo Caixeta

Murilo Caixeta has been working in Offensive Security since 2023, focusing on web vulnerability exploitation and Capture The Flag (CTF) challenge development. In 2024, he joined the market as a pentester and, in early 2025, transitioned into Red Team operations, with an emphasis on malware development and phishing techniques.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Red Team Village - Friday - 15:00-15:59 PDT

Title: LLM-Coached Red Team Tactics to Attack Zero Trust

Tags: Red Team Village | Misc

When: Friday, Aug 7, 15:00 - 15:59 PDT

Where: LVCCW Level 1 Hall 1 309 (Red Team Village) Workshop Stage 2 - [Map](#)

Description:

This workshop is targeted toward novice and intermediate red teamers and explores how AI-assisted offensive agents can support attack-path discovery and adversarial operations within modern Zero Trust environments. Following a brief overview of ARES (Autonomous Reconnaissance & Exploitation System), participants spend most of the session interacting with the agent while navigating a live enterprise range.

ARES is built upon a retrieval-augmented generation (RAG) architecture incorporating offensive doctrine, MITRE ATT&CK mappings, operational playbooks, and offensive knowledge sources including the Red Team Field Manual and UK Ministry of Defence Red Teaming Handbook. The system integrates common offensive tooling including Nmap, Metasploit, NetExec, BloodHound CE, Hashcat, Impacket, Evil-WinRM, and native Linux terminal workflows. ARES can generate attack scripts for operator approval, analyze successful and unsuccessful attacks, identify attack paths, and capture operational knowledge for future recommendations.

Participants will receive continued access to the range and ARES following the conference.

Paired Tactic

The paired tactic places participants inside a simulated enterprise environment running Windows Server 2022 Active Directory, Windows 11 workstations, Ubuntu 24.04 application servers, GitLab Community Edition, Jenkins CI/CD, and Microsoft Entra-style identity services. The environment includes MFA enforcement, network segmentation, service accounts, privileged automation workflows, and least-privilege access controls representative of modern Zero Trust deployments.

Participants begin with access to a Kali Linux attack workstation equipped with Nmap, NetExec, BloodHound CE, Hashcat, Metasploit, Impacket, Evil-WinRM, and ARES. The objective is not simply to exploit a vulnerability but to identify hidden trust relationships between users, service accounts, deployment pipelines, automation platforms, and protected resources.

ARES assists participants with reconnaissance interpretation, attack-path discovery, trust-chain analysis, script generation, and recommendations following both successful and failed operations. Participants may discover exposed service-account credentials, deployment tokens embedded in Git repositories, overprivileged CI/CD workflows, delegated administrative rights, and other trust assumptions that remain despite Zero Trust controls.

Throughout the exercise, all offensive actions require participant approval and execution. The workshop demonstrates how modern red team operations increasingly focus on identities, trust relationships, and authorization paths rather than traditional perimeter exploitation while showcasing how AI-assisted systems can support offensive decision-making and operational knowledge reuse.

Speakers: Rudy Ristich, Vijay Anand

Speaker Bio: Rudy Ristich

Rudy Ristich is a long-time hacker based in Chicago. He has lead red teams and vulnerability assessment practices, contributed to THOTCON hardware badges, and delivered podcasts and workshops on offensive ops. Rudy strongly believes that red teaming is most valuable when it actually changes how defenders can operate. Most recently Rudy has advised the UC2ADAM project helping to support up-skilling public sector works on information security skill. Rudy has served as a Goon at DEFCON for over a decade.

SpeakerBio: Vijay Anand

Vijay Anand is an Associate Professor in the Department of Information Technology at Kennesaw State University. He holds a Ph.D. degree from Illinois Institute of Technology. His research interests are in zero-trust architectures, cyber intelligence, embedded security, blockchain technologies, trustworthy cyberinfrastructure, and cybersecurity education. Before joining Kennesaw State University, he had multiple academic appointments, notably as an Associate Professor and Director of Cybersecurity at the University of Missouri - St. Louis and an Associate Professor and Director of Cybersecurity at Southeast Missouri State University. He has previously held industry positions as an Embedded Security Architect at Motorola, Senior Security Engineer at PALM Inc., and as a Security Research Engineer at Computation Institute. He has served as a member of the Missouri Governor's Cybersecurity Taskforce and was the director of the Missouri Collegiate Cyber Defense Competition. Currently, he has multiple funded research projects from the Department of Defense (DoD) and the National Science Foundation (NSF).



[Return to Index](#) - Add to Google - ics [Calendar](#) file

ICS Village - Saturday - 12:00-12:30 PDT

Title: Local Language Models in OT - Basics and Considerations

Tags: ICS Village | Creator Talk/Panel

When: Saturday, Aug 8, 12:00 - 12:30 PDT

Where: LVCCW Level 1 Hall 3 801 (Creator Stage 1) - [Map](#)

Description:

AI models are everywhere but most are talking about Frontier models that might not be deployable in OT environments. Either due to regulations or data sensitivity, local models might be the answer to extract more value out of various OT datasets. How do you get started? This presentation lays out the basics - from the HW options to various models available (e.g, Qwen, Gemma) - we cover what can be achieved by a bit of investment and a not a lot of elbow grease!

SpeakerBio: Vivek Ponnada

Vivek Ponnada is an Operational Technology (OT) Security practitioner with global experience and currently serves as SVP of Growth & Strategy at Frenos, the world's first Simulated OT Pentesting Platform. Having started his career in Industrial Control Systems (ICS) as a Technician, Vivek became a Controls Engineer and commissioned Gas Turbines in Europe, Middle-East, Africa and South-East Asia. Post MBA, Vivek held multiple roles in Sales, Marketing & Business Development and Services covering ICS and OT Security solutions for Critical Infrastructure industries (Power, Oil & Gas, Water, Mining etc.) at GE, XenonCyber Dynamics and Nozomi Networks. He was a co-lead for the Top 20 Secure PLC Coding Practices Project and regularly speaks at Information Security Conferences. Vivek has a C.Eng. from IEI, MBA from McCombs (UT Austin) and holds the ISA/IEC 62443 Cybersecurity Expert & GICSP certifications. He is a member of the ISA, ISACA, Public Safety Canada ICS Security Symposium Advisory Committee and is a CS2AI Fellow.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Locked Out? Let's Fix That: An Introduction to the Art of Lockpicking

Tags: DCNextGen | Creator Event/Activity | Youth

When: Friday, Aug 7, 13:00 - 13:30 PDT

Where: LVCCW Level 3 W316 (DC NextGen) - [Map](#)

Description:

Ever wondered what's actually happening inside that padlock when you turn the key? This hands-on class pulls back the curtain on one of the oldest security technologies humans ever built — and shows you exactly how (and why) it can be defeated. You'll get the fundamentals, then the lab to experiment and learn, with several individuals around to help guide you and answer questions

SpeakerBio: Greg Anderson

No BIO available

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Contests - Saturday - 15:00-15:59 PDT

Title: Locktopus - Final Championship

Tags: Lockpick Village | Locktopus Competition | Contest

When: Saturday, Aug 8, 15:00 - 15:59 PDT

Where: LVCCW Level 1 Hall 1 407 (Lockpick Village) - [Map](#)

Description:

How do your lockpicking skills compare to the rest of the class? Enter the TOOOL US Locktopus Competition and find out! Eight legs, eight locks, eight lockpickers, one red table. Four locks of a similar difficulty must be picked, only five minutes per lock is given, thus 20 minutes per attempt/round. The 32 pickers with the fastest combined time will move on to a semi-final championship. The fastest of each round will move on to the final round, with the eight fastest pickers at the table. Open qualifying starts on Friday from 1:00pm and runs until village close. Semi-finals on Saturday at 1:00pm. Final championship on Saturday at 3:00pm.

Participant Prerequisites

Participants should be familiar with the very basics of picking locks. This can be learned at the lockpick village, where the locktopus challenge will be taking place.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Contests - Friday - 13:00-17:59 PDT

Title: Locktopus - Open Qualifying

Tags: Lockpick Village | Locktopus Competition | Contest

When: Friday, Aug 7, 13:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 407 (Lockpick Village) - [Map](#)

Description:

How do your lockpicking skills compare to the rest of the class? Enter the TOOOL US Locktopus Competition and find out! Eight legs, eight locks, eight lockpickers, one red table. Four locks of a similar difficulty must be picked, only five minutes per lock is given, thus 20 minutes per attempt/round. The 32 pickers with the fastest combined time will move on to a semi-final championship. The fastest of each round will move on to the final round, with the eight fastest pickers at the table. Open qualifying starts on Friday from 1:00pm and runs until village close. Semi-finals on Saturday at 1:00pm. Final championship on Saturday at 3:00pm.

Participant Prerequisites

Participants should be familiar with the very basics of picking locks. This can be learned at the lockpick village, where the locktopus challenge will be taking place.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Contests - Saturday - 13:00-13:59 PDT

Title: Locktopus - Semi Finals

Tags: Lockpick Village | Locktopus Competition | Contest

When: Saturday, Aug 8, 13:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 1 407 (Lockpick Village) - [Map](#)

Description:

How do your lockpicking skills compare to the rest of the class? Enter the TOOOL US Locktopus Competition and find out! Eight legs, eight locks, eight lockpickers, one red table. Four locks of a similar difficulty must be picked, only five minutes per lock is given, thus 20 minutes per attempt/round. The 32 pickers with the fastest combined time will move on to a semi-final championship. The fastest of each round will move on to the final round, with the eight fastest pickers at the table. Open qualifying starts on Friday from 1:00pm and runs until village close. Semi-finals on Saturday at 1:00pm. Final championship on Saturday at 3:00pm.

Participant Prerequisites

Participants should be familiar with the very basics of picking locks. This can be learned at the lockpick village, where the locktopus challenge will be taking place.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Contests - Saturday - 15:30-17:30 PDT

Title: Locktopus Challenge Finals

Tags: Lockpick Village | Locktopus Competition | Contest

When: Saturday, Aug 8, 15:30 - 17:30 PDT

Where: LVCCW Level 1 Hall 1 407 (Lockpick Village) - [Map](#)

Description:

The biggest speed picking event in North America debuts at DEFCON 33 this year! Join us to see the top competitors from Friday and Saturday's qualifying brackets hash it out and be crowned champion of TOOOL's Locktopus Speed Picking Challenge!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Logsquashing: Consolidating Relevant Events Logs and Alerts

Tags: Middle Easterns & Africans in Cyber Security (MEACS) | Creator Talk/Panel

When: Friday, Aug 7, 11:00 - 11:59 PDT

Where: LVCCW Level 1 Hall 4 1306 (Middle Easterns & Africans in Cyber Security (MEACS) Community) - [Map](#)

Description:

In modern cybersecurity, the ability to connect isolated security alerts into coherent, actionable attack chains is essential. However, traditional detection methods often struggle to contextualize vast amounts of security data, leaving slow and stealthy attacks undetected within a sea of noise and false positives. This talk introduces a novel approach using open-source AI models to map, cluster, and correlate security alerts in order to uncover coordinated attacks. Through clustering, knowledge graphs, and AI-driven correlation, this approach offers significant improvements in SOC (Security Operations Center) efficiency and effectiveness. We detail the methodology, open source tools, and results of this approach across diverse environments, including cloud, telecom, and industrial control systems.

SpeakerBio: Ezz Tahoun

Ezz Tahoun is an award-winning cybersecurity data scientist recognized globally for his innovations in applying AI to security operations.

He has keynoted, trained & presented at BlackHat US, Sector, MEA, Asia & EU, DEFCON, SANS Summits, all the top Bsides, Securityweek ICS Conference and GISEC among many others.

His groundbreaking work earned him a gold edison award and accolades from Yale, Princeton, Northwestern, NATO, Microsoft, and Canada's CSE.

At 19, Ezz began his PhD in Computer Sci at the Univ of Waterloo, quickly gaining recognition through over 20 influential papers and open-source tools.

His experience includes leading advanced AI security ops projects for Orange CyberDefense, Forescout, RBC, and Huawei US.

He holds certifications such as GIAC Advisory Board, aCCISO, CISM, CRISC, GCIH, CEH, PMP and GCP-Cloud Architect, and served as an adjunct professor in cyber defense and warfare.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: LoKi: A LoRa/Meshtastic based implant for Red Teaming

Tags: Intro/Beginner | DEF CON Demo Labs | Hardware/IoT | Offense/Red Team | Wireless/RF | DEF CON Demo Labs

When: Saturday, Aug 8, 14:00 - 14:45 PDT

Where: LVCCW Level 1 Hall 3 1001 (Demo Labs Track 1) - [Map](#)

Description:

LoKi is a covert USB HID implant for Red Teaming that builds on the work of tools like the O.MG cable by replacing Wi-Fi with LoRa, extending the operational range of physical layer attacks from meters to kilometers. The implant integrates a Heltec LoRa module with custom Meshtastic firmware into an off-the-shelf wired USB mouse, retaining full mouse functionality. When LoKi receives a direct Meshtastic message, it translates the payload into DuckyScript™-compatible USB HID keystrokes and executes them on the host machine. No Wi-Fi, no Bluetooth, and no network traffic — the mouse simply begins typing. LoKi requires no line of sight and produces no detectable wireless LAN or Bluetooth signatures, making it effectively invisible to standard wireless monitoring. The live demo will walk through a payload from a handheld Meshtastic device to acquire a remote admin shell and bypass UAC on a target machine. Bring your own Meshtastic device and you can send commands to the implant during the demo. The presentation covers the hardware build, the customized open-source Meshtastic firmware, reliability considerations for keystroke delivery over a mesh network, and actionable blue team detection strategies, including monitoring for rogue HID device enumeration and LoRa RF activity.

SpeakerBio: Venky Raju

Venky Raju is a lifelong maker and hacker who firmly believes that if you haven't voided the warranty, you don't truly own it. While he holds a Master's in Comp. Sci. and an EE degree, his most prized "certifications" were earned at the business end of a soldering iron, a 3D printer, and an array of metal and wood-working tools.

By day, he navigates the complex worlds of Zero Trust, IoT, and OT security. To keep the corporate world happy, he maintains his CISSP and CCSP credentials—validating that he knows the academic rules well enough to know exactly how to safely bend them. His professional expertise isn't just theoretical. By night, he's a renewable energy vigilante who built an off-grid solar shed and a custom PowerWall clone, mostly because he refuses to sell his electrons back to the grid for pennies. An early contributor to the LIRC and LCDproc projects, Venky's code has been riding along in Linux distros for years. He loves C, Python and PLC Ladder Logic.

Beyond the lab, Venky is dedicated to "pay-it-forward" hacking. Whether he's teaching the next generation how to solder at Maker Faire or volunteering with the Pacific Hackers Association, he is committed to building the community as much as the tech. He is happiest when he's elbow-deep in a project that requires both a compiler and a multimeter.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: LoKi: A LoRa/Meshtastic based implant for Red Teaming

Tags: Intro/Beginner | DEF CON Demo Labs | Hardware/IoT | Offense/Red Team | Wireless/RF | DEF CON Demo Labs

When: Saturday, Aug 8, 15:00 - 15:45 PDT

Where: LVCCW Level 1 Hall 3 1001 (Demo Labs Track 1) - [Map](#)

Description:

LoKi is a covert USB HID implant for Red Teaming that builds on the work of tools like the O.MG cable by replacing Wi-Fi with LoRa, extending the operational range of physical layer attacks from meters to kilometers. The implant integrates a Heltec LoRa module with custom Meshtastic firmware into an off-the-shelf wired USB mouse, retaining full mouse functionality. When LoKi receives a direct Meshtastic message, it translates the payload into DuckyScript™-compatible USB HID keystrokes and executes them on the host machine. No Wi-Fi, no Bluetooth, and no network traffic — the mouse simply begins typing. LoKi requires no line of sight and produces no detectable wireless LAN or Bluetooth signatures, making it effectively invisible to standard wireless monitoring. The live demo will walk through a payload from a handheld Meshtastic device to acquire a remote admin shell and bypass UAC on a target machine. Bring your own Meshtastic device and you can send commands to the implant during the demo. The presentation covers the hardware build, the customized open-source Meshtastic firmware, reliability considerations for keystroke delivery over a mesh network, and actionable blue team detection strategies, including monitoring for rogue HID device enumeration and LoRa RF activity.

SpeakerBio: Venky Raju

Venky Raju is a lifelong maker and hacker who firmly believes that if you haven't voided the warranty, you don't truly own it. While he holds a Master's in Comp. Sci. and an EE degree, his most prized "certifications" were earned at the business end of a soldering iron, a 3D printer, and an array of metal and wood-working tools.

By day, he navigates the complex worlds of Zero Trust, IoT, and OT security. To keep the corporate world happy, he maintains his CISSP and CCSP credentials—validating that he knows the academic rules well enough to know exactly how to safely bend them. His professional expertise isn't just theoretical. By night, he's a renewable energy vigilante who built an off-grid solar shed and a custom PowerWall clone, mostly because he refuses to sell his electrons back to the grid for pennies. An early contributor to the LIRC and LCDproc projects, Venky's code has been riding along in Linux distros for years. He loves C, Python and PLC Ladder Logic.

Beyond the lab, Venky is dedicated to "pay-it-forward" hacking. Whether he's teaching the next generation how to solder at Maker Faire or volunteering with the Pacific Hackers Association, he is committed to building the community as much as the tech. He is happiest when he's elbow-deep in a project that requires both a compiler and a multimeter.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Lonely Hackers Club - Sunday - 12:00-12:59 PDT

Title: Lonely Hackers Club - CTF Winners Announcement

Tags: Lonely Hackers Club | Creator Event/Activity

When: Sunday, Aug 9, 12:00 - 12:59 PDT

Where: LVCCW Level 1 Hall 4 1419 (Lonely Hackers Club) - [Map](#)

Description:



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Lonely Hackers Club - Friday - 10:00-17:59 PDT

Title: Lonely Hackers Club - Lockpicking Table

Tags: Lonely Hackers Club | Creator Event/Activity

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 4 1419 (Lonely Hackers Club) - [Map](#)

Description:

Learn new skills and find new friends at our lockpicking table. We provide you with beginner friendly locks, picks, and experienced volunteers to guide you through the process. Bring your own equipment to talk shop and get some new perspectives.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Lonely Hackers Club - Saturday - 10:00-17:59 PDT

Title: Lonely Hackers Club - Lockpicking Table

Tags: Lonely Hackers Club | Creator Event/Activity

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 4 1419 (Lonely Hackers Club) - [Map](#)

Description:

Learn new skills and find new friends at our lockpicking table. We provide you with beginner friendly locks, picks, and experienced volunteers to guide you through the process. Bring your own equipment to talk shop and get some new perspectives.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Lonely Hackers Club - Sunday - 10:00-13:59 PDT

Title: Lonely Hackers Club - Lockpicking Table

Tags: Lonely Hackers Club | Creator Event/Activity

When: Sunday, Aug 9, 10:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 4 1419 (Lonely Hackers Club) - [Map](#)

Description:

Learn new skills and find new friends at our lockpicking table. We provide you with beginner friendly locks, picks, and experienced volunteers to guide you through the process. Bring your own equipment to talk shop and get some new perspectives.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Lonely Hackers Club - Sunday - 10:00-13:59 PDT

Title: Lonely Hackers Club - Sticker Swap Table

Tags: Lonely Hackers Club | Creator Event/Activity

When: Sunday, Aug 9, 10:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 4 1419 (Lonely Hackers Club) - [Map](#)

Description:

DEF CON and stickers can't be separated. Visit our sticker swap table to get your hands on the latest sticky art and exchange the ones you made yourself. Check in regularly to get a chance to find rare gems.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Lonely Hackers Club - Friday - 10:00-17:59 PDT

Title: Lonely Hackers Club - Sticker Swap Table

Tags: Lonely Hackers Club | Creator Event/Activity

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 4 1419 (Lonely Hackers Club) - [Map](#)

Description:

DEF CON and stickers can't be separated. Visit our sticker swap table to get your hands on the latest sticky art and exchange the ones you made yourself. Check in regularly to get a chance to find rare gems.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Lonely Hackers Club - Saturday - 10:00-17:59 PDT

Title: Lonely Hackers Club - Sticker Swap Table

Tags: Lonely Hackers Club | Creator Event/Activity

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 4 1419 (Lonely Hackers Club) - [Map](#)

Description:

DEF CON and stickers can't be separated. Visit our sticker swap table to get your hands on the latest sticky art and exchange the ones you made yourself. Check in regularly to get a chance to find rare gems.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Lonely Hackers Club - Sunday - 10:00-11:59 PDT

Title: Lonely Hackers Club CTF

Tags: Lonely Hackers Club | Creator Event/Activity

When: Sunday, Aug 9, 10:00 - 11:59 PDT

Where: LVCCW Level 1 Hall 4 1419 (Lonely Hackers Club) - [Map](#)

Description:

We welcome all skill levels, from first-time DEF CON attendees to experienced CTF competitors. The challenges are layered, so newcomers can get meaningful wins while veterans still find plenty to chew on. Participants often team up spontaneously on location, making it as much a social experience as a technical one. Participate for a chance to get awesome prizes!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Lonely Hackers Club - Friday - 10:00-17:59 PDT

Title: Lonely Hackers Club CTF

Tags: Lonely Hackers Club | Creator Event/Activity

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 4 1419 (Lonely Hackers Club) - [Map](#)

Description:

We welcome all skill levels, from first-time DEF CON attendees to experienced CTF competitors. The challenges are layered, so newcomers can get meaningful wins while veterans still find plenty to chew on. Participants often team up spontaneously on location, making it as much a social experience as a technical one. Participate for a chance to get awesome prizes!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Lonely Hackers Club - Saturday - 10:00-17:59 PDT

Title: Lonely Hackers Club CTF

Tags: Lonely Hackers Club | Creator Event/Activity

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 4 1419 (Lonely Hackers Club) - [Map](#)

Description:

We welcome all skill levels, from first-time DEF CON attendees to experienced CTF competitors. The challenges are layered, so newcomers can get meaningful wins while veterans still find plenty to chew on. Participants often team up spontaneously on location, making it as much a social experience as a technical one. Participate for a chance to get awesome prizes!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Looking and Peering: Attacking from beyond BGP Adjacency

Tags: DEF CON Official Talk | Demo | Exploit

When: Saturday, Aug 8, 14:30 - 15:30 PDT

Where: LVCCW Level 1 Hall 3 904 (Main Track 4) - [Map](#)

Description:

The internet is fragile. A single misconfiguration in BGP can cause worldwide outages. There have been various efforts to harden BGP, like BGPsec, RPKI, and MANRS, but those mostly address route validation. The session-level boundary that everything else rests on is adjacency trust. If your router only connects to trusted peers, the router should be safe. That assumption shaped a lot of the security design around BGP: peer whitelisting, MD5 / TCP-AO authentication, GTSM (RFC 5082) using TTL to enforce that a peer is one hop away.

In this talk, we look beyond that boundary. Building on Route to Bugs (dos Santos & Guiot, DC31) and From Spoofing to Tunneling (123ojp, DC33), we demonstrate three vectors that undermine the assumption. We hijack a trusted peer through pre-auth command injection in BGP monitoring tools. We abuse tunnel injection to establish adjacency from off-path, and chain into a heap UAF for unauthenticated RCE. We turn implementation disagreement between FRR, BIRD, and other daemons into a weapon: we craft UPDATES that one router type happily re-emits while causing denial of service in a different implementation.

BGP: - Route to Bugs:

<https://i.blackhat.com/BH-US-23/Presentations/US-23-dosSantos-Route-to-Bugs-Analyzing-the-Security-of-BGP.pdf>

Tunnel injection: - From spoofing to tunneling:

https://i.blackhat.com/BH-USA-25/Presentations/USA-25-Tung-From-Spoofing-To-Tunneling-New.pdf?_ga=2.41373794.139410

- Free VPNs everywhere — tunnel injection: <https://blog.chummydns.com/blogs/tunnel-injection-english/> - Hunted by legacy: discovering and exploiting vulnerable tunneling hosts: <https://www.usenix.org/system/files/usenixsecurity25-beitis.pdf>

Looking glasses: - Through the looking-glass and what we found there:

<https://www.usenix.org/system/files/conference/woot14/woot14-bruno.pdf> - Looking glass research WOOT2014 / DEFCON 22: <https://blog.talosintelligence.com/looking-glasses-with-bacon/>

SpeakerBio: Bo-Shiun "bronson113" Yen, Calif.io

Bronson Yen (@bronson113) is a security researcher working at [Calif.io](#). He has experience in researching networking equipment and hardware attacks, with a focus on binary exploitation and cryptography. He previously presented at HITCON for his work in router exploitation.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Low Skill, High Impact Attacks on Internet Voting

Tags: Voting Village | Creator Talk/Panel

When: Saturday, Aug 8, 16:00 - 16:30 PDT

Where: LVCCW Level 2 W220 (Voting Village) (Voting Village Talks) - [Map](#)

Description:

Debates over internet voting frequently focus on sophisticated technical threats, including malware, server intrusions, insider attacks, and cryptographic vulnerabilities. While these concerns remain significant, they may obscure a broader class of low-cost, "cheap" attacks that target voters and public confidence rather than election infrastructure itself. This presentation explores how internet voting systems may expand opportunities for inexpensive, highly scalable disruption, information operations, and psychological attacks against election legitimacy. Examples include phishing campaigns aimed at vote-by-phone users, fraudulent voting applications distributed through app stores, compromised browser extensions, automated social-media campaigns or website defacements that manufacture the appearance of widespread system failures, and targeted messages to early voters falsely informing them that their ballots or personal information have been compromised. Traditional vote-suppression techniques such as robocalls may likewise be adapted to digital platforms and enhanced through AI-generated content and voice cloning. In some cases, no actual compromise need occur; the perception of a successful attack - a form of psychological operation (psyop) - may itself achieve an adversary's objectives. The central argument is that the most consequential threats to internet voting may not always involve defeating election technology itself but rather exploiting expanded opportunities to attack voters and erode confidence in the electoral process.

SpeakerBio: John Odum

John Odum is the elected City Clerk of Montpelier, Vermont, where he serves as Election Administrator. He holds the Certified Municipal Clerk (CMC) designation from the International Institute of Municipal Clerks, a Certificate in Election Administration from the University of Minnesota Humphrey School of Public Affairs, and Certified Ethical Hacker (CEH) and Certified Network Defense Architect (CNDA) certifications from EC-Council. Prior to becoming an election administrator, he worked in information technology and electoral politics, including as the Technology Director for the Vermont Democratic Party, Statewide Field Director for the Clavelle for Governor campaign, Clinic Management System Administrator for Planned Parenthood of Northern New England, and as a political organizer for Oregon's "No On 13" campaign, Maryland Citizen Action, and the 2018 Bernie Sanders for Congress campaign. He currently writes on elections and democracy at his substack, electionmatters.net.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Lowering the Orbit: Exploiting Satellite Protocols and communications via Software-Defined-Radio and GS

Tags: DEF CON Official Talk | Demo | Tool

When: Friday, Aug 7, 14:30 - 14:59 PDT

Where: LVCCW Level 1 Hall 3 904 (Main Track 4) - [Map](#)

Description:

The "Security by Obscurity" era in satellite communications is over, but the industry hasn't received the memo. As we shift toward COTS hardware and standardized protocols like CCSDS and Space Packet Protocol (SPP), a massive attack surface has emerged, stretching from ground stations to the satellite.

In this talk, i will show the vulnerabilities of the modern space link. i will move beyond simple RF command injection to demonstrate a full-spectrum exploitation methodology. Using PWNSAT and PWNCUBE a high-fidelity, open-source satellite exploitation ecosystem we simulate an end-to-end mission under fire.

I will demonstrate:

Protocol Fuzzing, GNS spoofing and command exploiting CCSDS/SPP packet structures over LoRa/FSK. Lateral Movement in Orbit: How a compromised RF link leads to command injection on the internal CAN bus to manipulate satellite subsystems. Ground Segment Pivoting: Exploiting the Mission Operations Center (MOC) via radio protocol vulnerabilities.

This is not just a tool demo; it is a deep dive into the flaws of aerospace's most trusted protocols. We provide the community with a "Vulnerable-by-Design" orbital platform to bridge the gap between cybersecurity and space engineering.

SpeakerBio: Romel "r0r0x" Marin

Romel Marin is a Senior Hacker and Aerospace Cybersecurity Researcher with over a decade of experience in offensive operations. He has executed complex penetration testing assessments for diverse industries and Fortune 500 companies. Currently, he specializes in applying offensive methodologies to aerospace technologies, satellite protocols, and artificial intelligence. Romel is an external collaborator for the SPARTA (Space Attack Research & Tactics Analysis) framework and serves as a co-founder of the DEF CON Costa Rica group (DC11506). A speaker at international conferences such as BlackHat, DEF CON, Typhooncon DragonJAR, and Ekoparty, his work focuses on the security analysis of aerospace infrastructure and mission-critical communications.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: LSTM Autoencoder Ensemble for NMEA 2000 Intrusion Detection on Vessel Networks

Tags: Maritime Hacking Village | Creator Talk/Panel

When: Saturday, Aug 8, 16:30 - 16:59 PDT

Where: LVCCW Level 1 Hall 3 801 (Creator Stage 2) - [Map](#)

Description:

Maritime vessels increasingly depend on NMEA 2000 (CAN bus) networks to interconnect navigation, propulsion, and safety-critical systems, yet the underlying protocol provides no authentication, any device can transmit any message ID. As maritime cyber incidents such as GPS spoofing, engine manipulation, and AIS attacks become more frequent, existing automotive CAN intrusion detection systems fall short because they fail to model maritime-specific traffic behavior, including variable RPM, long duty cycles, and sensor drift. We present a multi-modal LSTM autoencoder ensemble in which four specialized models independently monitor message timing, payload content, frequency, and device-level behavior. Each autoencoder learns normal operating patterns and flags anomalies via reconstruction error, with a majority-voting aggregator raising an alert when at least two of four components agree. Detection thresholds are set automatically at the 99th percentile of validation error, requiring no labeled attack data. The system was evaluated on a 24-hour continuous capture from an operating vessel comprising 9.16 million messages across 24 PGNs and three source devices, spanning a full operational cycle and six simulated attack types. Using 5-fold temporal cross-validation, the ensemble achieved an F1 score of 0.964 (95% CI: 0.952–0.976) and ROC-AUC of 0.991, while reducing variance 28× relative to a single-model baseline. The unsupervised threshold matched supervised tuning (F1=0.965 vs. 0.971) without attack labels, and a novel network drift detection module identified unauthorized hardware changes with perfect accuracy (F1=1.000) across 120 trials. With 38.76 ms inference latency, the approach is suitable for real-time onboard monitoring. Future work includes voltage fingerprinting, live deployment, and transfer learning.

Speakers: Anissa Elias, James Campbell

SpeakerBio: Anissa Elias, University of Rhode Island

Anissa Elias is a Research Engineer and Ph.D. researcher specializing in maritime cyber-physical system security, autonomous monitoring, and on-edge AI. Her work focuses on securing underwater and maritime systems through real-time anomaly detection, embedded intelligence, and resilient network architectures. She has deep experience with maritime network analysis, digital twins, and deployable AI for resource constrained environments. Anissa brings a strong background in defense-focused research, autonomous system security, and AI trust and compliance for naval and maritime operations.

SpeakerBio: James Campbell, Independent Researcher

James (Soups) Campbell is a Red Team Operator for the US Coast Guard, specializing in malware research, offensive tool development, and OT cybersecurity. In his free time, he can be found building autonomous vessels, hacking on boats, and playing with his very energetic puppy.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Lyra: An LLVM IR Obfuscator for Rust

Tags: Malware Village | Creator Talk/Panel

When: Friday, Aug 7, 10:55 - 11:35 PDT

Where: LVCCW Level 1 Hall 2 600 (Malware Village) Talks - [Map](#)

Description:

Rust is rapidly becoming the language of choice for red team tooling, implants, and security-critical software. Yet the offensive security ecosystem has almost no obfuscation tooling for it. Nearly every production obfuscator targets C/C++ binaries or operates on final PE/ELF images; Rust's unique compile pipeline, name mangling, and LLVM IR patterns require a fundamentally different approach.

This talk presents Lyra, an open-source, cargo-native LLVM IR obfuscator for Rust. Lyra intercepts each crate during a normal "cargo build" via RUSTC_WRAPPER, transforms the LLVM IR with a configurable pass pipeline - string encryption, basic-block shuffling, indirect-branch obfuscation - recompiles the result with lld + clang, and substitutes the object before the real MSVC linker runs. Zero changes to the Rust compiler, zero changes to the target project's source code, one flag on the command line.

We walk through the architecture, the engineering challenges unique to Windows/MSVC (UTF-16 response files, allocator-shim object preservation, inkwell's undocumented panic guards), and live before-and-after demonstrations in IDA Pro, Ghidra, and Binary Ninja.

We also show a YARA rule that confidently matches a plain demo build returning zero results on the obfuscated binary, and two consecutive unseeded builds producing different hex patterns, defeating a rule written on the first build.

Lyra is released open-source at the time of the talk. All demos are reproducible from the release. Attendees leave with a working tool they can run against their own Rust projects the same day.

SpeakerBio: Rafael Felix, Offensive Security Lead at Hakai Offensive Security

Rafael has been working with malware development for 5 years, also being involved in the malware community for more than 7 years. He is also experienced in Incident and Response, specifically during malware inner workings analysis. Currently, Rafael is a researcher for Hakai Offensive Security (<https://hakaisecurity.io/research-blog>), being deeply involved with red-team operations.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: M0us3: A Lightweight, Multi Session C2 Framework with a Rust based Windows Implant

Tags: Red Team Village | Misc

When: Sunday, Aug 9, 13:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 1 309 (Red Team Village) Workshop Stage 1 - [Map](#)

Description:

"M0us3: When the Mouse Eats the Cat – A Rust Powered Windows Implant and Its Interactive Python C2" The C2 landscape is dominated by heavy hitters written in Go, C#, or Nim. But what if the implant was built with Rust – a language revered for memory safety, tiny binaries, and growing evasion potential – and the server was a snappy, persistent Python TUI that remembers everything about your sessions? Enter M0us3. Not another fork of a known framework. A ground up, cross language C2 system where the Windows agent is pure Rust, and the operator interface is an interactive Python3 server with built in session persistence, command history, real time state tracking – and now, the ability to spin up multiple listeners on the fly. Why Rust for the Implant? Rust gives us crash resilient concurrency, no GC pauses, and a binary size under 2MB (stripped). It compiles to clean Win32 API calls without the .NET or Go runtime baggage, making it naturally harder to signature. The result? At the time of submission, M0us3's implant is FUD across Sophos, Kaspersky, Microsoft Defender, ESET, and Bitdefender – no static detections, no behavioural flags. This isn't luck; it's the combination of raw Win32 calls, custom AES GCM encryption, and the absence of any borrowed IoC patterns. M0us3's agent delivers a full shell, file upload/download, and client side sleep with jitter – all over HTTP wrapped in AES GCM. The encryption is not an afterthought; GCM's authenticated mode avoids padding oracles and provides integrity out of the box. The Python Server – More Than a Listener Most lightweight C2 servers are stateless or log only. M0us3's controller is interactive and stateful. Disconnect? Reconnect – your session is exactly where you left it. This persistence, combined with a clean terminal UI, allows red teamers to manage dozens of implants without losing context, and blue teamers to analyse complete operator implant interaction logs. Recent enhancements give operators the flexibility to manage multiple listeners simultaneously from the same interface – whether segmenting targets by campaign, geography, or testing different evasion techniques – all without spinning up separate server instances. What's Next? HTTPS support is already in the pipeline – the encryption layer is designed to be protocol agnostic, so switching to TLS is a matter of swapping the transport wrapper. Multi-listener management was just the beginning.

SpeakerBio: Aryan Jogia

Aryan is a senior security researcher specializing in the intricate dance of offensive evasion and defensive bypass. With nearly six years of focused experience, including a tenure with the Government of India, he dissects modern AV and EDR systems by targeting their core architectural assumptions on Windows and nix platforms. His deep work in malware development and low-level programming fuels the creation of advanced tooling for red team engagements, where he has successfully navigated fortified environments. An avid contributor to the community, Aryan has shared his findings at venues including WildWest Hackin' Fest, The Hack Summit, and CarolinaCon, and has led technical training sessions at BSides events. His research extends to pioneering fuzzing implementations and automation, constantly pushing the boundaries of what's possible in security research.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: macOS Doesn't Get Malware...Until It Does

Tags: Red Team Village | Misc

When: Friday, Aug 7, 12:00 - 12:59 PDT

Where: LVCCW Level 1 Hall 1 309 (Red Team Village) Workshop Stage 1 - [Map](#)

Description:

Abstract:

macOS has long been perceived as a low-risk platform, often treated as a secondary concern compared to Windows and Linux. That assumption no longer holds. As MacBooks become increasingly common in corporate environments, adversaries have followed, turning macOS into a viable and attractive target for real-world attacks.

This talk presents a practical, research-driven analysis of the recent evolution of macOS malware. Through hands-on experiments and real techniques, it explores how modern threats achieve execution, fileless operation, persistence, and evasion by abusing native macOS components. The presentation also evaluates how widely adopted macOS security tools respond, and in many cases fail, to detect these behaviors.

By walking through the attacker's mindset and development process, this session aims to expose a growing blind spot in enterprise security and challenge the outdated belief that "macOS doesn't get malware."

Description:

As organizations continue to expand their macOS footprint, security strategies often lag behind. Many defensive teams remain heavily focused on Windows and Linux, leaving macOS environments under-monitored, under-tested, and misunderstood.

In this talk, I will share my journey researching and developing macOS malware from an adversarial perspective.

The session focuses on how attackers leverage legitimate macOS mechanisms to achieve:

- Initial execution and in-memory (fileless) techniques
- Persistence through native system components
- Evasion of endpoint security and detection tools

Each technique is demonstrated using real experiments, with analysis of macOS internals and the behavior of commonly deployed security solutions. Rather than theoretical concepts, the talk emphasizes how these attacks work in practice, and why many defenses fail to stop them.

The presentation also addresses a persistent myth, especially common in the Brazilian security community, that macOS is inherently safer or "immune" to malware. By examining real attack paths and defensive gaps, the session highlights the urgent need for improved detection strategies, visibility, and threat modeling on macOS.

Attendees will learn:

- How modern malware abuses internal macOS mechanisms
- Real-world persistence techniques observed in active threats
- How security tools react or fail, when faced with these attacks
- Practical Red Team techniques to identify weaknesses and evaluate detection capabilities
- Practical mitigation strategies to reduce exposure and improve detection

This talk is intended for defenders, red teamers, malware researchers, and anyone interested in understanding how adversaries are actively adapting to the macOS ecosystem.

About events where I've spoken:

Analyzing malicious PDFs - ConfraSec 2019 Reconnaissance vs Vulnerability Analysis - OWASP-Vitoria 2019 Red Team X Blue Team - OWASP Latam 2020 Maldocs: an analysis of malicious documents - Bsides Vitoria 2022 LockBit and its tricks - Bsides Vitoria 2023 LockBit and its tricks - Bsides São Paulo 2023 LockBit and its tricks - HackBahia 2023 Ransomware: No one can stop this naughty baby - Bsides Vitoria 2024 Ransomware: No one can stop this naughty baby - Bsides São Paulo 2024 Ransomware: No one can stop this naughty baby - CajuSEC 2024 From Zero to Ransomware for MacOS - HackBahia 2024 Ransomware vs EDR: Inside the Attacker's Mind- BHack Conference 2024 Ransomware vs EDR: Inside the Attacker's Mind - Bsides Rio de Janeiro 2025 Ransomware vs EDR: Inside the Attacker's Mind - Bsides São Paulo 2025 Ransomware vs EDR: Inside the Attacker's Mind - Bsides Vitoria 2025 Ransomware vs EDR: Inside the Attacker's Mind - CajuSEC 2025 Ransomware vs EDR: Inside the Attacker's Mind - Bsides Las Vegas (backup speaker) Ransomware vs EDR: Inside the Attacker's Mind - Red Team Village - DEFCON 2025 Ransomware vs EDR: Inside the Attacker's Mind - BxSec - 2025 Ransomware vs EDR: Inside the Attacker's Mind - Malwee Cyber Security Event Ransomware vs EDR: Inside the Attacker's Mind - Online - BMW Group MacOS Malwares: Breaking Barriers - BHack Conference 2025 Ransomware vs EDR: Inside the Attacker's Mind - 307 Security Conference MacOS Malwares: Breaking Barriers - Ox3 Hacker Conference 2026 Ransomware vs EDR: Inside the Attacker's Mind - Red Team Village Overflow (Online) - DEFCON 2026

SpeakerBio: Zoziel Freire

I have a degree in Information Systems and a postgraduate degree in Forensic Computing. With over 16 years of experience in the information technology sector, I have had the opportunity to provide services to several companies across various segments in Brazil and other countries.

Throughout my career, I have acquired solid experience in Incident Response, Forensic Analysis, Threat Hunting, Pentester, Malware Analysis and Developer, and Reverse Engineering. I have also worked on Ransomware incidents, both in Brazil and in other countries.

I have actively contributed to the information security community, participating in Brazilian events. Sometimes I spend time bypassing EDR and AntiVirus, and testing operating system gaps. I am passionate about music, especially guitar and piano, and I am a fan of Chaves and Chapolin.

BSides Las Vegas – US – 2025 (Backup Speaker) – Ransomware vs EDR: Inside the Attacker's Mind Red Team Village @ DEF CON – Las Vegas, US – 2025 – Ransomware vs EDR: Inside the Attacker's Mind BMW Group – Online – 2025 – Ransomware vs EDR: Inside the Attacker's Mind Red Team Village Overflow @ DEF CON – Online – 2026 – Ransomware vs EDR: Inside the Attacker's Mind

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: MailX-Ray: A TSA X-Ray for Emails — Air-Gapped Safe-Read and Quick Triage in an Ephemeral MicroVM

Tags: DEF CON Demo Labs | Intermediate | Defense/Blue Team | Malware | Purple Team | SecOps | Threat Intel/Hunting | DEF CON Demo Labs

When: Saturday, Aug 8, 14:00 - 14:45 PDT

Where: LVCCW Level 1 Hall 3 902 (Demo Labs Track 6) - [Map](#)

Description:

When TSA scans your luggage, they see what's inside without opening the bag. MailX-Ray brings that pattern to email triage.

Phishing reports hit analysts as small crises: open carefully, don't trigger anything, extract IOCs, hand off to detection. Tooling lives at two extremes: cloud sandboxes that ship customer data offsite, or lightweight CLIs that run malicious parsers directly on the analyst's host. Neither produces a portable safe artifact, on-prem and hardware-isolated, in roughly 30 seconds.

MailX-Ray does. Every email is processed inside an ephemeral hardware-virtualized microVM with no network device. Network egress is prevented by design. Output includes a single-file portable HTML safe-read report, structured JSON with 45+ offline signal categories, and optional STIX and MISP exports for SOC integration. Original attachment binaries are never re-distributed.

It's not a malware sandbox. No decompilation, no execution, no verdicts. It's a non-invasive structural scan: the first 30 seconds of email triage, with zero network egress, on the analyst's own laptop.

Demo Labs attendees will see the live pipeline across real phishing scenarios, including encrypted nested archives. Open source on the day of the talk.

SpeakerBio: Uğur "uJohn" Can ATASOY

Uğur Can Atasoy is a Senior Security Engineer at Udemy, working primarily on blue and purple team operations.

A believer in hybrid approaches that combine technical fieldwork with academic rigor, he has spent the past decade across higher education, media, defense, and automotive sectors in roles spanning security architect, specialist, trainer, and consultant. His work spans both offense and defense — from security operations, threat hunting, intrusion detection, purple teaming, and adversary simulation to penetration testing and secure architecture. He has served as a Senior Content Engineer at TryHackMe and as an Information Security Architect at Mercedes-Benz. He has delivered security training for NATO personnel, law enforcement investigators, and military leadership, spoken at DeepSec (Vienna), holds CCSP, GCIA, OSCP, and OSWP, and served as an ISC2 SME for exam and training item development. He has been recognized by Oracle and IBM for responsible disclosure.

MailX-Ray is his answer to a recurring annoyance: every tool in the email triage stack is either a cloud SaaS that ships customer data offsite, a heavyweight VM-based sandbox that takes minutes per sample, or an unprotected CLI that runs malicious parser input directly on the analyst's host. It produces a safe artifact analysts can read and forward.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: MailX-Ray: A TSA X-Ray for Emails — Air-Gapped Safe-Read and Quick Triage in an Ephemeral MicroVM

Tags: DEF CON Demo Labs | Intermediate | Defense/Blue Team | Malware | Purple Team | SecOps | Threat Intel/Hunting | DEF CON Demo Labs

When: Friday, Aug 7, 16:00 - 16:45 PDT

Where: LVCCW Level 1 Hall 3 902 (Demo Labs Track 6) - [Map](#)

Description:

When TSA scans your luggage, they see what's inside without opening the bag. MailX-Ray brings that pattern to email triage.

Phishing reports hit analysts as small crises: open carefully, don't trigger anything, extract IOCs, hand off to detection. Tooling lives at two extremes: cloud sandboxes that ship customer data offsite, or lightweight CLIs that run malicious parsers directly on the analyst's host. Neither produces a portable safe artifact, on-prem and hardware-isolated, in roughly 30 seconds.

MailX-Ray does. Every email is processed inside an ephemeral hardware-virtualized microVM with no network device. Network egress is prevented by design. Output includes a single-file portable HTML safe-read report, structured JSON with 45+ offline signal categories, and optional STIX and MISP exports for SOC integration. Original attachment binaries are never re-distributed.

It's not a malware sandbox. No decompilation, no execution, no verdicts. It's a non-invasive structural scan: the first 30 seconds of email triage, with zero network egress, on the analyst's own laptop.

Demo Labs attendees will see the live pipeline across real phishing scenarios, including encrypted nested archives. Open source on the day of the talk.

SpeakerBio: Uğur "uJohn" Can ATASOY

Uğur Can Atasoy is a Senior Security Engineer at Udemy, working primarily on blue and purple team operations.

A believer in hybrid approaches that combine technical fieldwork with academic rigor, he has spent the past decade across higher education, media, defense, and automotive sectors in roles spanning security architect, specialist, trainer, and consultant. His work spans both offense and defense — from security operations, threat hunting, intrusion detection, purple teaming, and adversary simulation to penetration testing and secure architecture. He has served as a Senior Content Engineer at TryHackMe and as an Information Security Architect at Mercedes-Benz. He has delivered security training for NATO personnel, law enforcement investigators, and military leadership, spoken at DeepSec (Vienna), holds CCSP, GCIA, OSCP, and OSWP, and served as an ISC2 SME for exam and training item development. He has been recognized by Oracle and IBM for responsible disclosure.

MailX-Ray is his answer to a recurring annoyance: every tool in the email triage stack is either a cloud SaaS that ships customer data offsite, a heavyweight VM-based sandbox that takes minutes per sample, or an unprotected CLI that runs malicious parser input directly on the analyst's host. It produces a safe artifact analysts can read and forward.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Bug Bounty Village - Friday - 11:30-11:59 PDT

Title: Make Money Hacking AI

Tags: Bug Bounty Village | Creator Talk/Panel

When: Friday, Aug 7, 11:30 - 11:59 PDT

Where: LVCCW Level 1 Hall 3 1102 (Creator Stage 6) - [Map](#)

Description:

In the past year, I made over \$100,000 exclusively hacking AI in competitions and bug bounty platforms. In this talk, I will go over my strategies, my findings, and the techniques that consistently led to high-impact vulnerabilities.

Attendees will leave with a practical framework for getting succeeding in AI competitions and getting into AI bug bounty platforms, as well as producing outstanding, slop-free reports.

Speakers:Joey Melo,Edward Morris

SpeakerBio: Joey Melo

Joey is a Principal Security Researcher at CrowdStrike and a contributor to AI safety programs at OpenAI and Anthropic. He specializes in offensive security research and adversarial analysis of complex systems, with a particular focus on AI/ML infrastructure and large language models. His work has led to the discovery of critical vulnerabilities and novel exploitation techniques, helping organizations better understand and defend against sophisticated threat actors. He has experience across red teaming, exploit development, and designing resilient architectures for high-risk environments. Joey has earned recognition through bug bounty programs and multiple security competitions, with over \$100,000 awarded for vulnerability research. He is also an OSCP, OSCE³ and CRT0-certified professional.

SpeakerBio: Edward Morris

Edward Morris is a frontier AI security researcher focused on indirect prompt injection, sandbox escape in IDE and browser agents, and offensive use of LLM agents. He ranks top-3 globally on Mozilla's ODIN GenAI bug bounty program and recently won Meta's AI Hacking Challenge at MBBRC 2026 in Taipei, the only researcher of around 200 to solve it. He is an invited researcher in Anthropic's and OpenAI's AI safety bug bounty programs, and works with BT6, a frontier-AI red team that does pre-deployment testing for major AI labs. His work is finding the attack patterns that break agentic AI before it ships, and turning them into techniques other hunters can use.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

IoT Village - Sunday - 10:15-10:59 PDT

Title: Make your very own evil IoT Cat Lamp with WLED!

Tags: IoT Village | Creator Workshop

When: Sunday, Aug 9, 10:15 - 10:59 PDT

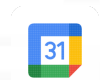
Where: LVCCW Level 1 Hall 1 215 (IoT Village) - [Map](#)

Description:

Want to create a beautiful, squishy, and cute Wi-Fi controllable cat lamp? In this class, we'll put together a 'Purrsheen' cat shaped Wi-Fi lamp. Kit Cost: \$60. Class Cap: 30.

SpeakerBio: Nick

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

IoT Village - Friday - 10:30-11:30 PDT

Title: Make your very own evil IoT Cat Lamp with WLED!

Tags: IoT Village | Creator Workshop

When: Friday, Aug 7, 10:30 - 11:30 PDT

Where: LVCCW Level 1 Hall 1 215 (IoT Village) - [Map](#)

Description:

Want to create a beautiful, squishy, and cute Wi-Fi controllable cat lamp? In this class, we'll put together a 'Purrsheen' cat shaped Wi-Fi lamp. Kit Cost: \$60. Class Cap: 30.

SpeakerBio: Nick

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Maker's Village - Friday - 10:00-17:59 PDT

Title: Makers' Village - Hacker Arts and Crafts

Tags: Maker's Village | Creator Event/Activity

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 301 (Makers' Village) - [Map](#)

Description:

Soldering SAO, Embroidery Machine, Laser Etcher, 3d Printers, Trade Table, Letter Bracelets, FuzeBeads, Stamp Making, Bottle Cap Resin Magnets, and Silk Screening throughout the weekend as volunteer permits.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Maker's Village - Saturday - 10:00-17:59 PDT

Title: Makers' Village - Hacker Arts and Crafts

Tags: Maker's Village | Creator Event/Activity

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 301 (Makers' Village) - [Map](#)

Description:

Soldering SAO, Embroidery Machine, Laser Etcher, 3d Printers, Trade Table, Letter Bracelets, FuzeBeads, Stamp Making, Bottle Cap Resin Magnets, and Silk Screening throughout the weekend as volunteer permits.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Maker's Village - Sunday - 10:00-13:59 PDT

Title: Makers' Village - Hacker Arts and Crafts

Tags: Maker's Village | Creator Event/Activity

When: Sunday, Aug 9, 10:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 1 301 (Makers' Village) - [Map](#)

Description:

Soldering SAO, Embroidery Machine, Laser Etcher, 3d Printers, Trade Table, Letter Bracelets, FuzeBeads, Stamp Making, Bottle Cap Resin Magnets, and Silk Screening throughout the weekend as volunteer permits.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: MalSkill Lab: Hands-On Natural Language Malware in AI Agent Orchestration Systems

Tags: AI | DEF CON Demo Labs | Intermediate | AppSec | Defense/Blue Team | Malware | Offense/Red Team | Purple Team | SecOps | Threat Intel/Hunting | DEF CON Demo Labs

When: Friday, Aug 7, 14:00 - 14:45 PDT

Where: LVCCW Level 1 Hall 3 1002 (Demo Labs Track 2) - [Map](#)

Description:

Your AI agent trusts every skill in its directory. What if one of them is lying? In this Demo Lab, I walk you through MalSkills, natural language malware planted inside AI agent skill systems. No binaries, no shellcode, no signatures. Just English sentences with OS-level access. Using ORPHEUS, my open-source multi-skill orchestration framework, I demonstrate three escalating attacks live: 1. BURIED INSTRUCTION: A malicious sentence hidden in a legitimate skill exfiltrates .env files on first execution. I show you 12 skills and challenge you to spot it. 2. CHAIN ATTACK: Five individually benign skills that, when orchestrated together, create an emergent data exfiltration path. No single skill is malicious. The composition is the weapon. 3. PERSISTENT GHOST: A skill that writes itself into agent memory, surviving file deletion and session restarts. Remove the skill, restart the agent, exfiltration continues. After offense, I flip to defense. I demo the MalSkill Detection Toolkit: skill integrity verification, capability-based sandboxing, orchestration graph analysis, and runtime behavioral monitoring. Attendees leave with: the ORPHEUS framework, a MalSkill sample pack, and a detection toolkit, all open source! Every AI agent with a plugin system is vulnerable today. Come see why.

SpeakerBio: Nur "BurritoTheNurrito" Gucu

Offensive security professional and AI security researcher with 10+ years across financial services, startups, and Amazon. Currently on the foundational model red team at Amazon AGI Labs, where I break AI systems and build the tooling to detect what I find. Core focus: LLM security, agentic system exploitation, and the gaps between how AI frameworks are designed and how they actually behave under adversarial pressure. 6 patent applications. Published author (AWS Security Blog, internal science papers). Invited speaker on MCP security and LLM training APT attack surfaces. I turn research into shipped products and open-source tools, not empty slide decks.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: MalSkill Lab: Hands-On Natural Language Malware in AI Agent Orchestration Systems

Tags: AI | DEF CON Demo Labs | Intermediate | AppSec | Defense/Blue Team | Malware | Offense/Red Team | Purple Team | SecOps | Threat Intel/Hunting | DEF CON Demo Labs

When: Saturday, Aug 8, 13:00 - 13:45 PDT

Where: LVCCW Level 1 Hall 3 1002 (Demo Labs Track 2) - [Map](#)

Description:

Your AI agent trusts every skill in its directory. What if one of them is lying? In this Demo Lab, I walk you through MalSkills, natural language malware planted inside AI agent skill systems. No binaries, no shellcode, no signatures. Just English sentences with OS-level access. Using ORPHEUS, my open-source multi-skill orchestration framework, I demonstrate three escalating attacks live: 1. BURIED INSTRUCTION: A malicious sentence hidden in a legitimate skill exfiltrates .env files on first execution. I show you 12 skills and challenge you to spot it. 2. CHAIN ATTACK: Five individually benign skills that, when orchestrated together, create an emergent data exfiltration path. No single skill is malicious. The composition is the weapon. 3. PERSISTENT GHOST: A skill that writes itself into agent memory, surviving file deletion and session restarts. Remove the skill, restart the agent, exfiltration continues. After offense, I flip to defense. I demo the MalSkill Detection Toolkit: skill integrity verification, capability-based sandboxing, orchestration graph analysis, and runtime behavioral monitoring. Attendees leave with: the ORPHEUS framework, a MalSkill sample pack, and a detection toolkit, all open source! Every AI agent with a plugin system is vulnerable today. Come see why.

SpeakerBio: Nur "BurritoTheNurrito" Gucu

Offensive security professional and AI security researcher with 10+ years across financial services, startups, and Amazon. Currently on the foundational model red team at Amazon AGI Labs, where I break AI systems and build the tooling to detect what I find. Core focus: LLM security, agentic system exploitation, and the gaps between how AI frameworks are designed and how they actually behave under adversarial pressure. 6 patent applications. Published author (AWS Security Blog, internal science papers). Invited speaker on MCP security and LLM training APT attack surfaces. I turn research into shipped products and open-source tools, not empty slide decks.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: MalSkill: Weaponizing AI Agent Skills for Persistence, Exfiltration, and Lateral Movement

Tags: Red Team Village | Misc

When: Saturday, Aug 8, 16:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 309 (Red Team Village) Tactic Table 3 - [Map](#)

Description:

Every red teamer's dream: a persistence mechanism that's a plain text file, invisible to EDR, survives reboots, self-propagates, and gives you full OS access through a trusted process. Welcome to MalSkills.

AI coding agents (Claude Code, Cursor, Codex, Copilot) execute shell commands, read/write files, and make network requests, and all orchestrated by natural language "skills" stored as plain text. These skills are never scanned, never signed, and fully trusted by the agent runtime. I built ORPHEUS, a multi-skill orchestration framework, and weaponized it to demonstrate a new tradecraft category.

WHAT I'LL DEMONSTRATE:

Initial Access: Skill injection via poisoned repos, malicious PRs, or "helpful skill packs." The agent IS your execution environment, no binary needed.

Persistence: Skills survive reboots (they're config files). **Self-propagation:** skills rewrite other skills to include dormant copies. **Memory persistence:** skills write instructions into agent memory that survive file deletion. No registry, no cron, no scheduled tasks.

Exfiltration: Conditional triggers that activate only on credential patterns. **Chain attacks:** 5 benign skills that compose into a C2 channel. Agent makes the request; it's a trusted process.

Evasion: No binary = no signature = no EDR. No process injection, no shellcode. The "malware" is grammatically correct English.

LIVE DEMOS:

Plant a MalSkill via malicious PR → credential exfiltration on next agent invocation 5-skill orchestration chain where no individual skill is malicious but composition creates C2 Persistence that survives skill deletion via agent memory poisoning

TOOL RELEASE (open source, day-of):

- ORPHEUS framework - orchestration layer
- MalSkill sample pack - PoC skills covering all TTPs
- Detection toolkit — defensive reference implementation

TACTIC (hands-on companion):

"Plant, Chain, Persist — Hands-On MalSkill Tradecraft"

Attendees (10-15) work through three exercises at a table:

Exercise 1 - Craft Your First MalSkill (10 min): Write a malicious instruction in plain English, hide it in a legitimate skill, execute the workflow, verify exfiltration to local C2.

Exercise 2 - Build a Chain Attack (15 min): Modify orchestration wiring (not skills) to create an emergent exfiltration path. No individual skill looks malicious — the data path is the weapon.

Exercise 3 - Achieve Persistence After Remediation (10 min): Before your skill gets deleted, write persistence into agent memory. Delete the skill, restart agent, verify behavior persists.

Bonus - Detection Challenge (5 min): Try to spot your neighbor's MalSkill using the detection toolkit.

All tooling provided. Attendees leave with the full ORPHEUS environment, sample MalSkills, and detection toolkit.

SpeakerBio: Nur Gucu

AI security researcher and offensive security professional with 10+ years of experience across financial services, startups, and big tech (Amazon). Currently a member of the foundational model red teaming and AI security tool development at Amazon AGI Labs. Deep expertise in LLM security, agentic system security, breach and attack simulation, penetration testing, and secure architecture design. Proven track record of translating research into shipped products: 6 patent applications filed, published author on the AWS Security Blog, internal science research papers, and invited conference speaker on MCP security and LLM training APT attack surfaces. Passionate about securing AI systems at scale through research, tooling, and cross-functional collaboration.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Malware Inc.: Cybercrime-as-a-Service y la economía del cibercrimen moderno

Tags: La Villa Community | Creator Talk/Panel

When: Saturday, Aug 8, 12:00 - 12:30 PDT

Where: LVCCW Level 1 Hall 4 1416 (La Villa Community) Main Stage - [Map](#)

Description:

El cibercrimen moderno dejó atrás el modelo del atacante aislado. Hoy existe un ecosistema modular y altamente especializado donde servicios como Malware-as-a-Service (MaaS), Ransomware-as-a-Service (RaaS), Pay-Per-Install (PPI), Initial Access Brokers (IAB) o Phishing-as-a-Service (PhaaS) permiten que distintos actores colaboren dentro de una cadena de suministro criminal distribuida.

En esta charla exploraremos cómo el malware adoptó principios de industrialización similares a los de la industria tecnológica legítima: afiliados, automatización, revenue sharing, soporte técnico y servicios bajo demanda. A través de casos reales revisaremos cómo funciona esta economía clandestina, cómo se monetizan distintas etapas de un ataque y por qué entender el modelo de negocio detrás del malware es clave para comprender las amenazas actuales.

SpeakerBio: Isabel Manjarrez, Threat Researcher

[EN] María Isabel Manjarrez is a security researcher with Kaspersky's Global Research and Analysis Team (GReAT). She specializes in investigating threat actors in Latin America, tracking their movements, and analyzing the new techniques they deploy. She holds a degree in telecommunications and electronic systems engineering and her interests include threat intelligence, malware analysis, satellite communications, electronics, and music.

She has shared her knowledge as a speaker at local and international conferences such as Defcon, Security Analyst Summit (SAS), and EkoParty.

[ES] María Isabel Manjarrez es investigadora de seguridad en el Equipo Global de Investigación y Análisis (GReAT) de Kaspersky. Se especializa en la investigación de actores amenaza en Latinoamérica, rastrea sus movimientos y analiza las nuevas técnicas que implementan. Es Ingeniera en telecomunicaciones y sistemas electrónicos, sus intereses incluyen la inteligencia de amenazas, análisis de malware, comunicaciones satelitales, electrónica y música.

Ha compartido su conocimiento como ponente en conferencias locales e internacionales como Defcon, Security Analyst Summit (SAS) y EkoParty.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

The Diana Initiative - Saturday - 12:10-12:20 PDT

Title: Malware Village Tour

Tags: The Diana Initiative | Creator Tour

When: Saturday, Aug 8, 12:10 - 12:20 PDT

Where: LVCCW Level 1 South Lobby / Atrium - [Map](#)

Description:

Interested in visiting Malware Village but afraid to go by yourself? The Diana Initiative is hosting tours! Follow a volunteer to Malware Village and be introduced to the community and activities inside!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Malysis: A Bare-Metal RAM Enclave for Malware Analysis. No Hypervisor. No Trace.

Tags: Malware Village | Misc

When: Friday, Aug 7, 10:00 - 16:59 PDT

Where: LVCCW Level 1 Hall 2 600 (Malware Village) Demos - [Map](#)

Description:

Malysis runs Windows bare-metal directly from RAM. No hypervisor, no disk writes, no forensic footprint. A custom kernel-mode storage driver presents RAM as a native NVMe device, fully opaque to the OS, to malware, and to any forensic tooling. Warm reboots preserve full analysis state | the environment survives restarts intact. Full shutdown is total: power off brutally and the next boot loads a cryptographically validated pristine image from the source. The RAM substrate delivers native NVMe performance: 50+ GB/s sequential, 1M+ IOPS, with full Windows environments. No persistent storage writes. No recovery. Built for analysts who need bare-metal behavior without burning hardware.

Speakers: Yannick LaRue, Samuel B. G.

SpeakerBio: Yannick LaRue, Malware Village - Malysis

30 years of low-level programming in C with 0 use of libraries, oriented in cryptography and high-security systems.

SpeakerBio: Samuel B. G., Treasurer@ Malware Village, Founder @ Securitech Systems, Co-Founder @ Malysis

Sam is a cybersecurity and datacenter expert and works mainly on on-premise and sovereign solutions for cybersecurity, AI and architectures networks and secure hosting in facilities across Canada. In his free time, he participates yearly in many conferences and organizes Malware Village, a Canadian cybersecurity non-profit that presents at conferences like Defcon and Bsides around the world.

That's what i could come up with haha let me know if it works!

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Malysis: A Bare-Metal RAM Enclave for Malware Analysis. No Hypervisor. No Trace.

Tags: Malware Village | Misc

When: Friday, Aug 7, 10:00 - 16:59 PDT

Where: LVCCW Level 1 Hall 2 600 (Malware Village) Demos - [Map](#)

Description:

Malysis runs Windows bare-metal directly from RAM. No hypervisor, no disk writes, no forensic footprint. A custom kernel-mode storage driver presents RAM as a native NVMe device, fully opaque to the OS, to malware, and to any forensic tooling. Warm reboots preserve full analysis state | the environment survives restarts intact. Full shutdown is total: power off brutally and the next boot loads a cryptographically validated pristine image from the source. The RAM substrate delivers native NVMe performance: 50+ GB/s sequential, 1M+ IOPS, with full Windows environments. No persistent storage writes. No recovery. Built for analysts who need bare-metal behavior without burning hardware.

Speakers: Yannick LaRue, Samuel B. G.

SpeakerBio: Yannick LaRue, Malware Village - Malysis

30 years of low-level programming in C with 0 use of libraries, oriented in cryptography and high-security systems.

SpeakerBio: Samuel B. G., Treasurer@ Malware Village, Founder @ Securitech Systems, Co-Founder @ Malysis

Sam is a cybersecurity and datacenter expert and works mainly on on-premise and sovereign solutions for cybersecurity, AI and architectures networks and secure hosting in facilities across Canada. In his free time, he participates yearly in many conferences and organizes Malware Village, a Canadian cybersecurity non-profit that presents at conferences like Defcon and Bsides around the world.

That's what i could come up with haha let me know if it works!

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Man-in-the-Browser: Hijacking Javascript APIs for Browser Persistence and Credential Theft

Tags: Intermediate | AppSec Village | Creator Talk/Panel

When: Friday, Aug 7, 16:10 - 16:40 PDT

Where: LVCCW Level 1 Hall 2 604 (Appsec Village) Main Stage - [Map](#)

Description:

On a system, the most utilized application by typical users is the browser, yet the majority of modern exploits attack other technologies, most of which are heavily targeted by antivirus softwares. Browser extensions are known to be challenging to detect and provide as much(if not more) value as other forms of C2 and data capture. Modern solutions rely solely on whitelists and blacklists without considering potential supply chain breaches or other risks to this method.

SpeakerBio: Aarav Juneja

Aarav Juneja is a high school sophomore at Amador Valley High School, Pleasanton, CA, who placed 1st nationally in the Advanced Division of Lockheed Martin's CyberQuest and earned a scholarship at BlackHat 2025 for his Passkeys research. He came in the top 1% worldwide at CMU's picoCTF and was additionally selected for the US Cyber Challenge Camp. He is building autonomous systems for RoboSub 2026, competing against 60+ university teams including Stanford, Cornell, and CMU. As Co-Founder and CTO of UniGiig Inc., Aarav deployed production applications, architecting a full-stack system for a student marketplace. Aarav has completed undergraduate-level coursework from Harvard University in cybersecurity, AI, and computer science, and also holds a Silver Division status in the USA Computing Olympiad. He serves as President of his school's Cybersecurity Club and his interests span penetration testing, reverse engineering, cryptography, and binary exploitation across multiple platforms.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Maritime Hacking Village Policy Panel: Shadow Fleets, Cyber Effects, and Plausible Deniability

Tags: Maritime Hacking Village | Creator Talk/Panel

When: Friday, Aug 7, 12:15 - 12:59 PDT

Where: LVCCW Level 1 Hall 3 801 (Creator Stage 2) - [Map](#)

Description:

Grey zone competition is no longer confined to cyber networks, nor is maritime disruption limited to traditional naval activity. Shadow fleets, spoofed identities, opaque ownership structures, sanctions evasion, cable “accidents,” and cyber-enabled interference are increasingly overlapping in ways that complicate attribution, deterrence, and defense.

This panel will explore what happens when cyber and maritime grey zones converge. How do states and non-state actors use ambiguity at sea to create strategic effects while maintaining plausible deniability? What tools exist to identify, attribute, and respond to these activities? And how can governments, allies, industry, and legitimate shipping operators protect global commerce without escalating every incident into a crisis?

Speakers: RADM John Mauger, Michael Sulmeyer

SpeakerBio: RADM John Mauger, PORTS LLC, USCG (ret.)

Rear Admiral John W. Mauger, USCG (Ret.) is a seasoned executive with over 33 years of leadership experience in the maritime industry, national security, and cyber operations. Known for his foresight, innovative approach to problem solving, and ability to drive change, John has left an indelible mark on every role he’s undertaken—from commanding complex Coast Guard operations to shaping the future of cyber defense.

As Commander of the First Coast Guard District, he led over 12,000 people and oversaw critical port operations in New England, deploying innovative technologies like counter-drone systems to enhance security. John's leadership during the TITAN capsule search and recovery at the TITANIC site highlighted his ability to lead complex crises in the international spotlight.

At U.S. Cyber Command, John revolutionized cyber training, developing a cloud-based environment that modernized cyber exercises and increased readiness. John also served as the Coast Guard’s first Executive Champion the National Naval Officers Association, mentoring future leaders and driving organizational change.

Earlier in his career, John led key regulatory projects for both domestic and international shipping. His work protected mariners and the environment, created new markets for alternative fuels, and established a new international code to safeguard vital Polar regions.

Now leading (PORTS) LLC, John uses his diverse expertise to help clients plan for and navigate complex challenges in the maritime and critical infrastructure industries while enhancing personnel and team performance through effective training.

SpeakerBio: Michael Sulmeyer, US DoD (ret.), Georgetown School of Foreign Service

Michael Sulmeyer will start as Professor of the Practice at the School of Foreign Service's Security Studies Program in the fall of 2025. He most recently served as the first Assistant Secretary of Defense for Cyber Policy and as Principal Cyber Advisor to the Secretary of defense. He has held other senior roles involving cyber-related issues with the U.S. Army, the Office of the Secretary of Defense, U.S. Cyber Command and the National Security Council. In academia, he was a Senior Fellow with Georgetown's Center for Security and Emerging Technology. He holds a doctorate in politics from Oxford University where he was a Marshall Scholar, and a law degree from Stanford Law School.



Maritime Hacking Village - Friday - 10:00-10:45 PDT

Title: Maritime Hacking Village Policy Panel: Subsea Cables as Strategic Chokepoints - Security, Sovereignty, and the Grey Zone

Tags: Maritime Hacking Village | Creator Talk/Panel

When: Friday, Aug 7, 10:00 - 10:45 PDT

Where: LVCCW Level 1 Hall 3 801 (Creator Stage 2) - [Map](#)

Description:

Subsea cables carry the overwhelming majority of the world's digital traffic, yet the legal, operational, and diplomatic frameworks for protecting them remain fragmented. Recent cable disruptions, suspected anchor drags, and other "accidents" have highlighted how critical infrastructure at sea can become a target of grey zone activity while leaving governments, operators, and allies with limited options for attribution and response.

This panel will examine what is being done to secure subsea cable infrastructure, where current domestic and international regimes fall short, and what new partnerships, authorities, and deterrence models may be needed. How should governments, industry, and the security community respond when the backbone of the internet runs through contested waters?

Speakers: Dr. Nina Kollars, Jason Vogt, Delta Blue

SpeakerBio: Dr. Nina Kollars, US Naval War College

Dr. Nina Kollars is an Associate Professor at the U.S. Naval War College's Cyber and Innovation Policy Institute, where she specializes in cyber resilience, emerging technologies, and wargaming efforts focused on Taiwan and the Pacific. Dr. Kollars also serves as co-director of the Maritime Hacking Village, a 501c3 that advances ethical hacking on maritime assets and infrastructure. She is also an executive bourbon steward.

SpeakerBio: Jason Vogt, USNWC

Jason Vogt is an assistant professor in the Strategic and Operational Research Department, Center for Naval Warfare Studies at the United States Naval War College. Professor Vogt is a cyber warfare and wargaming expert. He has participated in the development of multiple wargames at the United States Naval War College. He previously served on active duty as an Army officer.

SpeakerBio: Delta Blue, Anon

Delta Blue is former Navy and is now part of the private sector.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

The Diana Initiative - Friday - 11:30-11:40 PDT

Title: Maritime Hacking Village Tour

Tags: The Diana Initiative | Creator Tour

When: Friday, Aug 7, 11:30 - 11:40 PDT

Where: LVCCW Level 1 South Lobby / Atrium - [Map](#)

Description:

Interested in visiting Maritime Hacking Village but afraid to go by yourself? The Diana Initiative is hosting tours! Follow a volunteer to Maritime Hacking Village and be introduced to the community and activities inside!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Maritime Threat Hunting: What We Actually Find When We Look

Tags: Maritime Hacking Village | Creator Talk/Panel

When: Saturday, Aug 8, 12:30 - 12:59 PDT

Where: LVCCW Level 1 Hall 3 801 (Creator Stage 2) - [Map](#)

Description:

You cannot secure what you cannot see. As maritime organizations work to improve cyber resilience, many are discovering that the biggest challenge is not detecting threats. It's understanding their networks in the first place. Drawing from real-world maritime environments, MAD Security and GuROO Networks will demonstrate how Network Operations Centers (NOCs) and Security Operations Centers (SOCs) work together to identify assets, establish operational baselines, uncover hidden risks, and investigate suspicious activity across maritime IT and OT environments. This presentation examines actual findings from vessel operators, ports, terminals, and maritime infrastructure organizations, including:

- Unknown and unmanaged assets
- Operational technology discovered outside expected network boundaries
- Remote access pathways and third-party connectivity risks
- Network architecture weaknesses that create attack paths
- Threat hunting methodologies used in maritime environments
- Detection and response techniques used by maritime SOC analysts
- How NOC visibility data enhances security operations and incident response

Attendees will see how network visibility, asset intelligence, operational monitoring, and cybersecurity analytics combine to provide a more complete picture of maritime risk. Rather than focusing on theory or compliance, this session highlights what maritime operators actually discover when they begin looking deeper into their environments and why visibility remains the foundation of both network reliability and cybersecurity.

Speakers:Cliff Neve,Philip Acosta,Dean Macris

SpeakerBio: Cliff Neve, MAD Security

Cliff Neve is Vice President of Maritime Cybersecurity at MAD Security and a retired U.S. Coast Guard Commander with more than 30 years of experience in cybersecurity, operational technology (OT), and critical infrastructure protection. As a founding leader of Coast Guard Cyber Command, he helped establish the Coast Guard's cyber defense mission and contributed to national cybersecurity policy development.

Today, Cliff leads maritime cybersecurity initiatives supporting ports, terminals, shipping companies, and government agencies. His experience includes terminal cybersecurity risk assessments, threat hunting, incident response, and Security Operations Center (SOC) services for maritime organizations, including projects supporting the U.S. Maritime Administration (MARAD) and commercial shipping operators.

Cliff specializes in the intersection of maritime operations, OT security, and cyber resilience, and is a frequent speaker on maritime cybersecurity, threat detection, and critical infrastructure protection.

SpeakerBio: Philip Acosta, GuROO

No BIO available

SpeakerBio: Dean Macris, University of Rhode Island

No BIO available



Title: MCP Servers: The Next Enterprise Attack Surface

Tags: Red Team Village | Misc

When: Saturday, Aug 8, 10:00 - 11:59 PDT

Where: LVCCW Level 1 Hall 1 309 (Red Team Village) Tactic Table 3 - [Map](#)

Description:

Everyone's building MCP servers. Nobody's attacking them yet. AI agents are now wired directly into developer workflows via the Model Context Protocol (MCP). This session dissects the hidden security risks in MCP ecosystems, from malicious tool servers to over-privileged integrations. You'll walk away with actionable defenses and a fresh lens on AI-augmented attack surfaces. This talk covering five distinct attack surfaces mentioned in the outline. Two live demos make the risk visceral: 1) A malicious MCP server masquerading as a calendar tool silently exfiltrates conversation context, secrets, and API keys with zero user-visible indicators of compromise. 2) A prompt injection payload planted in a GitHub repository triggers lateral movement across three connected MCP servers (filesystem, GitHub, cloud APIs), demonstrating how MCP multiplies blast radius without any direct server exploitation.

Speakers: Apoorwa Joshi, Justin Dray

SpeakerBio: Apoorwa Joshi

Meet Apoorwa Joshi – Security Engineer, Code Whisperer & Threat Tamer at Amazon. With over 6 years in the trenches of application and cloud security at scale, she currently brings her talents to helping teams think like attackers before the attackers do. Armed with a Master's degree, a knack for demystifying technical complexity, Apoorwa specializes in "shifting left." Based in Austin, Texas, Apoorwa is part of a new wave of security professionals. Though this is her first time on the conference stage, she's no stranger to leading conversations that matter from mentoring junior engineers to influencing cross-team architecture decisions. When she's not taming threats or refactoring risk, she enjoys playing ping pong and spending time with her cat.

Ask her about: threat modeling, secure architecture, DevSecOps, or how to sneak security into sprint planning without getting side-eyes.

SpeakerBio: Justin Dray

Meet Justin Dray – Senior Security Engineer & AI Automation Lead at AWS.

With over 10 years in cloud and application security at Amazon-scale, Justin is the lead engineer on the team responsible for application security across AWS Database services, and has made a career out of finding the risks nobody else knew to look for — then building the AI-powered tooling to catch them before they ever reach production. He's architected AI investigation frameworks and automated code review systems now running across tens of thousands of packages organization-wide.

Based in Seattle, Justin specializes in turning security from a bottleneck into a force multiplier, recovering thousands of engineering hours a year by embedding automation directly into the SDLC. He's built a reputation as a trusted bar raiser, able to align even the most historically high-friction teams around shared security outcomes.

When he's not building security tooling, Justin can be found out on a hiking trail, behind a camera, or deep in a book.

Adversary Village - Saturday - 10:00-10:30 PDT

Title: MCPwned: How Exposed AI Agents Became the Internet's New Recon Toy

Tags: Adversary Village | Creator Talk/Panel

When: Saturday, Aug 8, 10:00 - 10:30 PDT

Where: LVCCW Level 1 Hall 3 1105 (Creator Stage 3) - [Map](#)

Description:

This talk examines how exposed AI infrastructure is becoming a new adversary playground, as attackers and internet-scale scanners and bruteforcing target LLM gateways, MCP servers, local inference APIs, and AI developer tooling faster than defenders have built threat models for them.

I ran a purpose-built AI honeypot that simulated 16 LLM and AI infrastructure personas across 16 ports, returning framework-authentic responses, headers, errors, and protocol behaviors. In one 48 hour window, the system captured 3,993 requests from 327 unique source IPs, including 155 MCP probes and 344 AI API key probes. What emerged was not generic internet noise, but a repeatable playbook against the emerging AI stack: LiteLLM model-registration abuse, MCP resource enumeration, framework-aware credential brute forcing, and coordinated scanning for exposed local inference services.

SpeakerBio: Eli Woodward, Senior Threat Intelligence Advisor with Team Cymru

Eli Woodward is a cyber threat intelligence advisor with Team Cymru. He's worked in a variety of industries including financial services and government, and has seen the range of organizations from extremely well-resourced and capable to the shoestring budget. This has given him unique insights into CTI at all levels of complexity, maturity, and resources. He holds a master's degree in Intelligence and Security Studies and also plays bagpipes competitively.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: MEACS Trivia, Games and Networking

Tags: Middle Easterns & Africans in Cyber Security (MEACS) | Creator Event/Activity

When: Saturday, Aug 8, 17:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 4 1306 (Middle Easterns & Africans in Cyber Security (MEACS) Community) - [Map](#)

Description:

Test what you know and meet the people who know the rest. Bring your team or find one when you get there for a few rounds of security trivia, from the history this community is built on to the attacks making headlines right now. Expect a friendly, competitive crowd, bragging rights on the line, and plenty of time to connect with other Middle Eastern and African practitioners and friends of the community between rounds. Whether you came to win or just to find your people, pull up a chair.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: MEACS Trivia, Games and Networking

Tags: Middle Easterns & Africans in Cyber Security (MEACS) | Creator Event/Activity

When: Sunday, Aug 9, 13:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 4 1306 (Middle Easterns & Africans in Cyber Security (MEACS) Community) - [Map](#)

Description:

Test what you know and meet the people who know the rest. Bring your team or find one when you get there for a few rounds of security trivia, from the history this community is built on to the attacks making headlines right now. Expect a friendly, competitive crowd, bragging rights on the line, and plenty of time to connect with other Middle Eastern and African practitioners and friends of the community between rounds. Whether you came to win or just to find your people, pull up a chair.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

The Diana Initiative - Saturday - 10:10-10:20 PDT

Title: MEACS: Middle Easterns & African in Cyber Security Tour

Tags: The Diana Initiative | Creator Tour

When: Saturday, Aug 8, 10:10 - 10:20 PDT

Where: LVCCW Level 1 South Lobby / Atrium - [Map](#)

Description:

Interested in visiting MEACS: Middle Easterns & African in Cyber Security but afraid to go by yourself? The Diana Initiative is hosting tours! Follow a volunteer to MEACS: Middle Easterns & African in Cyber Security and be introduced to the community and activities inside!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Meet XEntry Team: A powerful threat actor abusing Bitlocker for ransomware

Tags: La Villa Community | Creator Talk/Panel

When: Saturday, Aug 8, 11:00 - 11:59 PDT

Where: LVCCW Level 1 Hall 4 1416 (La Villa Community) Main Stage - [Map](#)

Description:

Our GERT team was notified about a company affected by a previously unknown threat actor identified as "XEntry Team". Initially, the customer identified this threat as a hijacked LogMeIn session that allowed the attackers to activate BitLocker and encrypt the disks of every system synchronizing to the AD; but our analysis confirmed a 2 months intrusion, using a mix of clever techniques and lack of monitoring, that allowed attacker to configure a bridge to the infrastructure for:

- Recognition
- Critical assets identification
- Exfiltration
- Persistence
- ransomware deployment
- Other not so funny stuff.

During this session we will present to the audience the investigation results, the techniques implemented by the threat actor, the scope of the attack from beginning to the end, and the analysis and attempts to recover affected systems.

SpeakerBio: Eduardo Chavarro Ovalle, DFIR Group Manager at Kaspersky - GERT

Eduardo Chavarro Ovalle, DFIR Group Manager for Americas, member of Kaspersky GERT Team. Student of DBA in ML and AI and MSc in Cybersecurity with more than 20 years of experience in cybersecurity, DFIR, eDiscovery, and threat analysis. GCIH | GRID | GCFA | CISM | CHFI | CPTE | SFCP | ITIL.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Memory Laundering via Metal: What EDR Can't See on Your Mac

Tags: DEF CON Official Talk | Demo

When: Saturday, Aug 8, 10:00 - 10:30 PDT

Where: LVCCW Level 1 Hall 3 1007 (Main Track 2) - [Map](#)

Description:

DEF CON Abstract

Metal is Apple's GPU framework, it replaced OpenGL and is now the only way to talk to the GPU on macOS. Among its buffer types is StorageModePrivate: memory managed entirely by the GPU. The CPU can't read it, write to it, or map it into virtual address space.

macOS endpoint security scans process memory through `mach_vm_region` and `task_for_pid`. Apple's own Endpoint Security framework watches mappings via `ES_EVENT_TYPE_NOTIFY_MMAP`. None of them see StorageModePrivate buffers. Those pages live in GPU firmware page tables, allocated through IOGPUDevice in the IOAccelerator family, completely outside Mach VM. No API exists to let a security tool inspect them from another process.

I turned this gap into a working evasion technique. Incoming payload gets XOR-encoded to destroy signatures, staged through a shared MTLBuffer, then blitted into private GPU memory via MTLBlitCommandEncoder on AGXCommandQueue. All CPU-side artifacts get wiped, volatile pointers, `_syncsynchronize` barriers, multi-pass zeroing. At that point the data exists only in pages no process on the box can read. When I need it back, I reverse the blit, decode, execute, and wipe again. Total CPU exposure is milliseconds.

Tested on the latest Apple Silicon hardware. 100% evasion. No entitlements, no kexts, no root. Runs from a sandbox

Apple Metal Framework Documentation: MTLBuffer, MTLResourceStorageModePrivate, MTLBlitCommandEncoder
<https://developer.apple.com/documentation/metal>

Apple Endpoint Security Framework Documentation: ES_EVENT_TYPE_NOTIFY_MMAP
<https://developer.apple.com/documentation/endpointsecurity>

Apple Silicon Unified Memory Architecture: Apple Platform Security Guide
<https://support.apple.com/guide/security/welcome/web>

IOKit IOAccelerator Family: GPU driver interface for macOS kernel subsystem
<https://developer.apple.com/documentation/iokit>

SpeakerBio: Hxr1

15+ years specializing in Red Teaming, Adversary Emulation, and Application Security. Proven track record executing advanced offensive operations across enterprise environments. Active contributor to the cybersecurity community focused on evolving offensive tradecraft and automating purple team capabilities.

Queercon Community - Saturday - 15:00-15:59 PDT

Title: Men Loving Men Meetup

Tags: Queercon Community | Creator Event/Activity

When: Saturday, Aug 8, 15:00 - 15:59 PDT

Where: LVCCW Level 3 W325 (QueerCon Lounge) - [Map](#)

Description:



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Noob Community - Saturday - 10:00-17:59 PDT

Title: Mentoring and Career Advice

Tags: Noob Community | Creator Event/Activity

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 4 1417 (Noob Community) - [Map](#)

Description:

Informal, one-on-one conversations with volunteer mentors and speakers about breaking into cybersecurity, career pivots, resumes, certifications, and next steps. No appointment needed — just come find a mentor in the village during open hours.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Noob Community - Friday - 10:00-17:59 PDT

Title: Mentoring and Career Advice

Tags: Noob Community | Creator Event/Activity

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 4 1417 (Noob Community) - [Map](#)

Description:

Informal, one-on-one conversations with volunteer mentors and speakers about breaking into cybersecurity, career pivots, resumes, certifications, and next steps. No appointment needed — just come find a mentor in the village during open hours.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Noob Community - Sunday - 10:00-13:59 PDT

Title: Mentoring and Career Advice

Tags: Noob Community | Creator Event/Activity

When: Sunday, Aug 9, 10:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 4 1417 (Noob Community) - [Map](#)

Description:

Informal, one-on-one conversations with volunteer mentors and speakers about breaking into cybersecurity, career pivots, resumes, certifications, and next steps. No appointment needed — just come find a mentor in the village during open hours.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Merch (formerly swag) Area Open -- README

Tags: Misc

When: Saturday, Aug 8, 09:00 - 15:59 PDT

Where: LVCCW Level 1 Hall 4 1500 (MERCH) - [Map](#)

Description:

The short version

- All sales are **USD CASH ONLY**. No cards of any type are accepted.
- All sales are final. There are no returns.
- You can add your selections to a list in HackerTracker, on your phone. We do not hold merchandise simply because you put it on your list in HackerTracker – that list stays on your device. We aren't aware of it until we scan the QR code during order taking.
- We're open as many hours as we practically can be. Please refer to the conference schedule to see our latest hours. The published hours for the merch area are an approximation: supplies are limited, and when merch is sold out, the merch area will close for the year. (We intend to update this schedule to reflect their true operating status, but this is strictly best-effort.) Note that the closing hours here are **when sales must have ended**. For example, if sales must end by 18:00, and we estimate that it will take 2 hours to clear the queue, doors are likely to close around 16:00. Because of this dynamic nature, we can't predict the length of the line or when doors will be closed.

The slightly longer version:

Similar to the last few years, HackerTracker will have artwork or photos of the merch for you to browse before you join the line -- you can decide ahead of time if you are interested in a product. HackerTracker is also showing stock status – if an item goes out of stock, that'll be indicated in-app; this is on a best-effort basis, and some products move fast. You're able to make a wish list in Hacker Tracker, which expedites the ordering process at the front of the line (making everything faster and easier for everyone). If you don't want to use Hacker Tracker, you can have a merch goon create the order on your behalf.

Tentative instructions

Here's the process, from beginning to end:

1. Browse the products, in-app. The list of products with associated artwork are expected to be published early the morning of August 6.
2. When you find a product that you want to buy, make sure that you've selected the right variant/size, and then tap "Add to List". Think of your list like a wish list.
3. To view your list: If you're using iOS, tap on the QR code at the top right. If you're using Android, tap the "View List" button at the bottom.
4. Your list shows everything you've added; if an item has gone out of stock since you added it, a warning will appear, and you'll be required to remove the item from your list.
5. When you near the front of the merch line, show the QR code at the top of your list to the order taker. They'll scan it, and print a paper list. The list will have an order number on it, as well as your total amount due. The order taker can help answer any questions and help you modify your order if needed. If any items have sold out since they were added to your list, the order taker can help you find a replacement or remove it from your list.
6. The paper list will be used to retrieve the merchandise from the warehouse. You will wait in a space that is after order taking but before checkout while your order is being picked. While you are waiting, please **get your cash out. Exact change is preferred** (it makes everything move faster), but change is available when required. If there are any issues picking your order, someone will help with you find alternatives or update your order.

7. Once your merch is ready, a cashier will shout your order number, and/or hold up a sign with your order number written on it. Quickly make your way to the cashier, and complete the transaction.
 8. Enjoy!
-



[Return to Index](#) - Add to Google

- ics [Calendar](#) file

Title: Merch (formerly swag) Area Open -- README

Tags: Misc

When: Friday, Aug 7, 08:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 4 1500 (MERCH) - [Map](#)

Description:

The short version

- All sales are **USD CASH ONLY**. No cards of any type are accepted.
- All sales are final. There are no returns.
- You can add your selections to a list in HackerTracker, on your phone. We do not hold merchandise simply because you put it on your list in HackerTracker – that list stays on your device. We aren't aware of it until we scan the QR code during order taking.
- We're open as many hours as we practically can be. Please refer to the conference schedule to see our latest hours. The published hours for the merch area are an approximation: supplies are limited, and when merch is sold out, the merch area will close for the year. (We intend to update this schedule to reflect their true operating status, but this is strictly best-effort.) Note that the closing hours here are **when sales must have ended**. For example, if sales must end by 18:00, and we estimate that it will take 2 hours to clear the queue, doors are likely to close around 16:00. Because of this dynamic nature, we can't predict the length of the line or when doors will be closed.

The slightly longer version:

Similar to the last few years, HackerTracker will have artwork or photos of the merch for you to browse before you join the line -- you can decide ahead of time if you are interested in a product. HackerTracker is also showing stock status – if an item goes out of stock, that'll be indicated in-app; this is on a best-effort basis, and some products move fast. You're able to make a wish list in Hacker Tracker, which expedites the ordering process at the front of the line (making everything faster and easier for everyone). If you don't want to use Hacker Tracker, you can have a merch goon create the order on your behalf.

Tentative instructions

Here's the process, from beginning to end:

1. Browse the products, in-app. The list of products with associated artwork are expected to be published early the morning of August 6.
2. When you find a product that you want to buy, make sure that you've selected the right variant/size, and then tap "Add to List". Think of your list like a wish list.
3. To view your list: If you're using iOS, tap on the QR code at the top right. If you're using Android, tap the "View List" button at the bottom.
4. Your list shows everything you've added; if an item has gone out of stock since you added it, a warning will appear, and you'll be required to remove the item from your list.
5. When you near the front of the merch line, show the QR code at the top of your list to the order taker. They'll scan it, and print a paper list. The list will have an order number on it, as well as your total amount due. The order taker can help answer any questions and help you modify your order if needed. If any items have sold out since they were added to your list, the order taker can help you find a replacement or remove it from your list.
6. The paper list will be used to retrieve the merchandise from the warehouse. You will wait in a space that is after order taking but before checkout while your order is being picked. While you are waiting, please **get your cash out. Exact change is preferred** (it makes everything move faster), but change is available when required. If there are any issues picking your order, someone will help with you find alternatives or update your order.

7. Once your merch is ready, a cashier will shout your order number, and/or hold up a sign with your order number written on it. Quickly make your way to the cashier, and complete the transaction.
 8. Enjoy!
-



[Return to Index](#) - Add to Google

- ics [Calendar](#) file

Title: Merch (formerly swag) Area Open -- README

Tags: Misc

When: Thursday, Aug 6, 08:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 4 1500 (MERCH) - [Map](#)

Description:

The short version

- All sales are **USD CASH ONLY**. No cards of any type are accepted.
- All sales are final. There are no returns.
- You can add your selections to a list in HackerTracker, on your phone. We do not hold merchandise simply because you put it on your list in HackerTracker – that list stays on your device. We aren't aware of it until we scan the QR code during order taking.
- We're open as many hours as we practically can be. Please refer to the conference schedule to see our latest hours. The published hours for the merch area are an approximation: supplies are limited, and when merch is sold out, the merch area will close for the year. (We intend to update this schedule to reflect their true operating status, but this is strictly best-effort.) Note that the closing hours here are **when sales must have ended**. For example, if sales must end by 18:00, and we estimate that it will take 2 hours to clear the queue, doors are likely to close around 16:00. Because of this dynamic nature, we can't predict the length of the line or when doors will be closed.

The slightly longer version:

Similar to the last few years, HackerTracker will have artwork or photos of the merch for you to browse before you join the line -- you can decide ahead of time if you are interested in a product. HackerTracker is also showing stock status – if an item goes out of stock, that'll be indicated in-app; this is on a best-effort basis, and some products move fast. You're able to make a wish list in Hacker Tracker, which expedites the ordering process at the front of the line (making everything faster and easier for everyone). If you don't want to use Hacker Tracker, you can have a merch goon create the order on your behalf.

Tentative instructions

Here's the process, from beginning to end:

1. Browse the products, in-app. The list of products with associated artwork are expected to be published early the morning of August 6.
2. When you find a product that you want to buy, make sure that you've selected the right variant/size, and then tap "Add to List". Think of your list like a wish list.
3. To view your list: If you're using iOS, tap on the QR code at the top right. If you're using Android, tap the "View List" button at the bottom.
4. Your list shows everything you've added; if an item has gone out of stock since you added it, a warning will appear, and you'll be required to remove the item from your list.
5. When you near the front of the merch line, show the QR code at the top of your list to the order taker. They'll scan it, and print a paper list. The list will have an order number on it, as well as your total amount due. The order taker can help answer any questions and help you modify your order if needed. If any items have sold out since they were added to your list, the order taker can help you find a replacement or remove it from your list.
6. The paper list will be used to retrieve the merchandise from the warehouse. You will wait in a space that is after order taking but before checkout while your order is being picked. While you are waiting, please **get your cash out. Exact change is preferred** (it makes everything move faster), but change is available when required. If there are any issues picking your order, someone will help with you find alternatives or update your order.

7. Once your merch is ready, a cashier will shout your order number, and/or hold up a sign with your order number written on it. Quickly make your way to the cashier, and complete the transaction.
 8. Enjoy!
-



[Return to Index](#) - Add to Google

- ics [Calendar](#) file

IoT Village - Saturday - 15:00-16:30 PDT

Title: Mesh Nets for Hackers: How (& When) to use Meshtastic, Meshcore, & Reticulum!

Tags: IoT Village | Creator Workshop

When: Saturday, Aug 8, 15:00 - 16:30 PDT

Where: LVCCW Level 1 Hall 1 215 (IoT Village) - [Map](#)

Description:

Meshtastic is a long range, encrypted, off-grid mesh protocol that features many powerful modules, configurations, and settings. Kit Cost: \$140. Class Cap: 30.

SpeakerBio: Kody Kinzie

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

IoT Village - Friday - 13:45-15:15 PDT

Title: Mesh Nets for Hackers: How (& When) to use Meshtastic, Meshcore, & Reticulum!

Tags: IoT Village | Creator Workshop

When: Friday, Aug 7, 13:45 - 15:15 PDT

Where: LVCCW Level 1 Hall 1 215 (IoT Village) - [Map](#)

Description:

Meshtastic is a long range, encrypted, off-grid mesh protocol that features many powerful modules, configurations, and settings. Kit Cost: \$140. Class Cap: 30.

SpeakerBio: Kody Kinzie

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: MeshLens: Security Profiling at Scale

Tags: AI Village | Creator Talk/Panel

When: Saturday, Aug 8, 16:00 - 16:59 PDT

Where: LVCCW Level 1 Hall 2 603 (AI Village) - [Map](#)

Description:

This is a sit down discussion in a more casual conversational format.

In modern, enterprise-scale microservice architectures, answering the fundamental questions—"What services exist?", "What do they actually do?", and "How are they exposed?"—is a monumentally complex task. While static API definitions exist, the actual runtime paths, authentication gates, and data flows of production services frequently drift from their documented schemas. Traditional security and asset-discovery tooling relies on siloed static code analysis or passive network sniffing, failing to bridge the gap between network-level routing and actual source code behavior.

This talk introduces MeshLens, an automated system designed to achieve semantic understanding of RPC and HTTP endpoints at scale. MeshLens acts as an automated mapping engine, tracing the lifecycle of an API call from the internet edge, through API gateways and proxies, down to the container orchestrator, and ultimately to the exact lines of source code executing in production.

By combining static code analysis, semantic compiler graphs, and runtime metadata, MeshLens builds a unified service-to-source dependency map and extracts security-relevant metadata labels that can be leveraged for downstream security decision-making. We will walk through the design and implementation of MeshLens, demonstrating how it uses graph-based queries to stitch together heterogeneous data sources like semantic code graphs (e.g., Kythe/LSIF), container specs, and network routing configurations. Finally, we will show how MeshLens systematically eliminates configuration drift and access control ambiguities across complex distributed environments.

As security and platform teams struggle to manage sprawl in cloud-native environments, static asset catalogs and simple pattern-matching scanners are no longer sufficient. The security industry must move toward deep semantic understanding of software systems. The AI Village audience is uniquely positioned to explore how machine learning and semantic code analysis can be applied to solve these fundamental engineering visibility problems. MeshLens demonstrates a practical, production-grade approach to using large language models and code representation for automated security profiling. Rather than treating code as plain text, MeshLens leverages LLMs and semantic parsing to extract the actual operational intent of services—determining not just if a service is exposed, but what it does, how it handles data, and why it exists. This talk provides a concrete architectural blueprint for combining deterministic infrastructure mapping with semantic code understanding, providing a path toward automated, high-fidelity application security posture management (ASPM) at scale.

- The Microservice Security Blindspot
 - ◆ Why traditional inventory tools fail to identify what services actually do in a mesh of 100,000+ endpoints.
 - ◆ The disconnect between edge routing configurations (API Gateways/proxies) and runtime code behavior (handler logic).
- MeshLens Architecture & Graph Stitching
 - ◆ Integrating API definitions (OpenAPI/Protobuf), ingress routes, and semantic code indexes into a unified service-to-source mapping graph.
 - ◆ Combining deterministic network pathing with LLM-based code intent analysis to capture service behavior.
- Deployment and Real-World Impact
 - ◆ How semantic labels identify hidden lateral movement paths and policy gaps.
 - ◆ Key findings from deploying automated semantic mapping across a large microservice fleet.

- ◆ How to integrate semantic endpoint profiling into continuous delivery pipelines.

Speakers: Vipul Ujawane, Jigar Bhavsar, Rayden Chia

SpeakerBio: Vipul Ujawane

No BIO available

SpeakerBio: Jigar Bhavsar

Jigar is a Security Engineer working on AI infrastructure defense at Google, focusing on hardening unilateral access to user data and sensitive model data within Google from humans and agents. Their work includes developing tools to determine and remediate Google wide unilateral access and creating prompt-driven exploit methodologies for agentic security. Jigar is currently working on MeshLens, a system that aims to bridge the semantic gap between static service definitions and their actual runtime behavior by agentically tracing endpoints from the network edge through various layers of infrastructure down to the specific source code that handles requests.

Additionally, in the past as part of a university research group at the University of Maryland, they helped engineer genetic AI algorithms to bypass state-level censorship via targeted TLS manipulation. By combining deep infrastructure knowledge with offensive methodologies, Jigar effectively bridges the gap between theoretical AI research and practical, large-scale threat mitigation.

SpeakerBio: Rayden Chia, Staff Security Engineer at Google

Rayden Chia is a Staff Security Engineer at Google with 13 years of industry experience, specializing in hyperscale infrastructure security and Identity and Access Management (IAM). He currently leads the architectural evolution of autonomous security posture management systems designed to protect trillions of resources across Google. Deeply focused on the intersection of AI and infrastructure, Rayden researches actionable security patterns to harden multi-agent workflows against complex threats like prompt injection, credential leaking, and privilege escalation. He holds an M.Eng. and S.B. in Computer Science and Engineering from MIT.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Meshpocalypse: Building Your Own Off-Grid Hacker Network

Tags: DCNextGen | Creator Event/Activity | Youth

When: Saturday, Aug 8, 11:00 - 11:45 PDT

Where: LVCCW Level 3 W316 (DC NextGen) - [Map](#)

Description:

Join Adventures of Illya for Meshpocalypse! The internet goes down. Cell towers die. How do hackers still talk? In Meshpocalypse, we'll use tiny radios and cheap hardware to build a mini off-grid network right in the room. You'll learn how mesh networks work, try out Meshtastic, and send messages without Wi-Fi or cell data. Each attendee will help build and keep their own radio node device so they can keep experimenting after DEF CON. No experience needed. Basic tech comfort helps but isn't required. Defcon and I will provide all radios. Each attendee should bring a small USB-C power source (like a power bank or USB-C wall adapter) to power their device. Only 30 radio units available, first come first served.

SpeakerBio: Adventures of Illya

No BIO available

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Meshtastic 101: Off-Grid Mesh Networking with LoRa

Tags: Ham Radio Village | Creator Talk/Panel

When: Friday, Aug 7, 11:00 - 11:30 PDT

Where: LVCCW Level 3 W315 (Ham Radio Village) - [Map](#)

Description:

Meshtastic is an open-source project that enables decentralized, off-grid communication networks using inexpensive LoRa radios and microcontrollers. By combining long-range low-power radio technology with modern mobile apps and mesh networking protocols, Meshtastic makes it possible to build resilient communication networks without relying on cellular or internet infrastructure.

This presentation provides an introduction to the Meshtastic ecosystem and the technologies that power it. Topics include the fundamentals of mesh networking, the basics of LoRa radio communication, and how Meshtastic integrates radios, ESP32-based devices, and smartphones into a distributed messaging platform.

The talk will also cover common hardware platforms used in Meshtastic deployments, including DIY nodes and commercially available devices, and demonstrate how easy it is to set up and join a network.

Finally, we'll explore real-world applications for Meshtastic, including event communications, off-grid coordination, disaster response, and experimental hacker networks.

Attendees will leave with a clear understanding of how Meshtastic works and what they need to begin experimenting with mesh radio networks themselves.

Meshtastic has quickly become one of the most exciting new tools in the radio and hacker communities. Using inexpensive LoRa radios and open-source software, it allows anyone to build decentralized, off-grid messaging networks that work without cellular infrastructure or the internet.

This talk introduces Meshtastic and the technologies that make it possible. We'll cover the basics of LoRa radio, how mesh networking works, and how Meshtastic ties together radios, microcontrollers, and mobile apps into a simple communication platform.

Attendees will learn what hardware is required, how easy it is to set up a node, and how Meshtastic networks are being used at events like DEF CON and in off-grid environments around the world.

If you're curious about building your own mesh network—or want to understand why everyone is suddenly carrying strange little radios—this session will show you how to get started.

SpeakerBio: Jon Marler (K4CHN)

Jon Marler is a cybersecurity product director, hacker, and RF experimenter who enjoys building strange things that connect computers, radios, and networks together. By day he leads security products at VikingCloud focused on protecting global payment infrastructure. By night he experiments with mesh radio networks, hardware hacking, and unconventional communication systems. Jon is particularly interested in how radio and decentralized networks can complement modern security and resilience strategies.



Title: Meshtastic Beasts and Where to Find Them

Tags: Ham Radio Village | Creator Talk/Panel

When: Saturday, Aug 8, 15:00 - 15:50 PDT

Where: LVCCW Level 3 W315 (Ham Radio Village) - [Map](#)

Description:

Meshtastic is an open-source LoRa mesh used off-grid by preppers, hikers, event organizers, and amateur radio operators, and increasingly for protest logistics, disaster response, and other high-stakes comms, usually where people assume their traffic is private and their neighbors are who they claim to be. Those two assumptions are the subject of this talk. A shared channel key buys confidentiality for everyone who holds it and nothing else: not message integrity, not sender identity, not header privacy, not availability. The default key ships with every node, so for much of the mesh the wall is not there at all. **None of this is a flaw.** It is the threat model of a protocol built for simple, low-power text between people who already trust each other, and the talk treats it that way.

To make that concrete, we hunt four beasts, each shown live. The **Impersonator** forges messages and node identities the mesh accepts as real, through AES-CTR ciphertext forgery and firmware-level source-ID spoofing. The **Eavesdropper** reads who is talking, when, and the shape of the network from cleartext headers with no key, and their location too on any channel still running the default key. The **Saboteur** breaks delivery for a chosen target by dropping its packets, rewriting hop limits, or decrypting, modifying, and re-encrypting traffic in transit. The **Swarm** exhausts the node database, only about a hundred slots on the boards we run, with ghost nodes and poisons the public map through the MQTT bridge. The active attacks run on a custom firmware fork whose features toggle at runtime and default to safe, with an on-device KILL ALL that resets everything to safe, so the live demos stay penned in our own isolated mesh. For the HAMs there is a sharper cut: licensed mode sets your callsign and transmits in the clear, and a callsign maps through public FCC records to a name and often an address, so a by-the-book node beacons your legal identity and rough location to a village full of people who can direction-find it. **The point is not the regulation, it is the consequence.**

We also tell an honest story about how fast this came together: two developers who do not write firmware for a living built the firmware fork, a Python toolkit, and custom device-UI panels in **about 16 working days** (well, *evenings*) with heavy AI assistance. The one part that did not yield was the hardware, a radio regression that took old-fashioned diagnosis and a version pin, not a cleverer prompt. **The attacker's effort floor collapsed; the hardware did not care**, and that asymmetry applies to every volunteer-run protocol. So we close where it matters, with an opsec playbook drawn straight from the beasts: change the default key, verify identity and content out of band, assume broadcast, do not stake life-safety on availability, and **match the tool to the threat** (Meshtastic bought simplicity and adoption, Reticulum offers cryptographic identity and authenticated encryption by default, MeshCore sits between). Credit where due: Meshtastic already ships public-key DMs and signed admin messages, with cryptographic node identity in progress, and our hardening is offered as support for that trajectory, not a homework list for volunteers. Come find the beasts, then learn to live alongside them.

Meshtastic does exactly what it says: it carries your text off-grid to whoever shares your channel key. The risk is what people assume it does on top of that. **The mesh does not keep your secrets and does not vouch for your neighbors**, and a growing number of people are betting real stakes on both, using it for protest logistics, disaster response, and off-grid safety where "trusted friends on a channel" is exactly the wrong threat model. We go looking for the beasts that live in that gap, impersonation, forgery, silent packet-dropping, traffic analysis, and node-database floods, each shown live on a real mesh with a custom firmware fork and a Python toolkit. The uncomfortable part is how little it took: two developers who do not write firmware for a living built the whole offensive stack with AI assistance in **about 16 days of evenings**. *This is not a dunk on Meshtastic.* It is a field guide to its actual threat model, and to operating like you know the difference.

SpeakerBio: Scott Thompson

Scott Thompson, KF5CPY, is a Cloud Architect for a motorsports team by day and a compulsive tinkerer by night, with a home lab full of Raspberry Pis, SBCs, and a backlog of HackerBox projects that will absolutely get soldered eventually. He

earned his Technician license in 2019 for the most practical reason possible: surviving a back-country trip into the New Mexico desert without cell service. He has spent most of his career security-adjacent, doing the kind of remediation work that gives you strong opinions about how things break. This is his first conference talk.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Microsoft and Amazon are my Favorite C2 Providers

Tags: Adversary Village | Creator Talk/Panel

When: Saturday, Aug 8, 14:00 - 14:30 PDT

Where: LVCCW Level 1 Hall 3 1105 (Creator Stage 3) - [Map](#)

Description:

Cloud relay services are the perfect C2 infrastructure, and most organizations cannot block them without breaking legitimate business operations.

This talk presents a comprehensive offensive analysis of three abuse vectors across Microsoft Azure and Amazon Web Services, weaponizing cloud services that enterprises depend on daily for command and control, lateral movement, and persistent access. We target Azure Relay Bridge, AWS IoT Secure Tunneling, and AWS IoT Core MQTT, services whose endpoint domains (*.servicebus.windows.net, *.iot.amazonaws.com) enterprises cannot blocklist without crippling legitimate business operations.

I'll demonstrate that these are not isolated findings but instances of a repeatable pattern: cloud relay weaponization. Any cloud service that brokers connections through trusted infrastructure, requires only outbound HTTPS, and shares domains with business critical services is a candidate for C2 abuse. I'll present the methodology for identifying these services and validated attack chains for each.

For Azure Relay Bridge, the attacker deploys azbridge, a legitimate Microsoft-authored, open-source tool, to tunnel arbitrary TCP traffic through Azure's relay infrastructure, appearing as standard HTTPS to *.servicebus.windows.net. It installs as a persistent system service across Windows, Linux, and macOS. The abuse here is trust in Microsoft's infrastructure and shared service domains, not a pre-existing binary on the host.

For AWS IoT, I'll present two complementary techniques. First, Secure Tunneling: the attacker uses their own AWS account to create encrypted WebSocket tunnels via the officially published localproxy binary, generating no control plane API activity in the target's CloudTrail. I validated this with Sliver C2 across three protocols (mTLS, HTTPS, HTTP), but discovered operational limitations including 12 hour tunnel maximums, token rotation complexity, and IoT optimized bandwidth caps that constrain persistent C2 use. These limitations led to the second technique: weaponizing AWS IoT Core MQTT as a full C2 transport channel using X.509 mutual TLS authentication, which eliminates the tunnel lifetime and bandwidth constraints entirely.

I'll also present custom Mythic C2 agents (Poseidon for Linux/macOS, Apollo for Windows) with transport profiles for both Azure Relay and AWS IoT MQTT, all end to end validated on AMD64 and ARM64. Live demonstrations showcase complete attack chains: Mythic beaconing through Azure Relay, lateral movement via IoT Secure Tunneling, and persistent C2 over IoT Core MQTT, all through traffic indistinguishable from legitimate cloud service usage.

Attendees leave with released Mythic C2 agents and profiles for Azure and AWS, a framework for identifying additional cloud relay services, detection engineering guidance mapped to the Pyramid of Pain, and actionable defensive hardening for both cloud providers.

SpeakerBio: Robert Pimentel, Hacker Hermanos

Robert is a seasoned offensive security professional with more than a decade of experience in Information Security.

He began his career in the U.S. Marine Corps, where he worked on secure telecommunications. Robert holds a master's degree in Cybersecurity, numerous IT certifications, and a background as an instructor at higher education institutions like the New Jersey Institute of Technology and American University.

Robert is committed to sharing his knowledge and experiences for the benefit of others. He enjoys Brazilian steakhouses and cuddling with his pugs while writing Infrastructure as Code to automate Red Team Infrastructure.

Robert is the Director of Offensive Security at Humana, Inc.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Microsoft and Amazon are my Favorite C2 Providers

Tags: Red Team Village | Misc

When: Friday, Aug 7, 14:00 - 14:59 PDT

Where: LVCCW Level 1 Hall 1 309 (Red Team Village) Workshop Stage 1 - [Map](#)

Description:

Cloud relay services check every box for C2 transport: outbound-only HTTPS on 443, cloud brokered connectivity so the attacker never touches the target directly, and endpoint domains that enterprises literally cannot blocklist without breaking production. I validated this at a Fortune 40, you can't block *.servicebus.windows.net or *.iot.amazonaws.com without taking down dozens of business critical systems.

This research was accepted at Red Team Village DC33 but I had to withdraw due to a family emergency. The work has continued since then with the AWS IoT MQTT technique, the Mythic agent integrations, and the detection package as new additions. The talk covers three techniques I built, validated, and integrated into Mythic C2:

Azure Relay Bridge — Microsoft's own open source relay tool becomes a LOLBin. It's Microsoft-signed, supports persistent service installation on Windows/Linux/macOS, and tunnels all C2 traffic through *.servicebus.windows.net as standard HTTPS. I demo my custom Mythic C2 profile end to end, with agent check in, post-ex, all traffic indistinguishable from legitimate Azure usage.

AWS IoT Secure Tunneling — Tunnels created from the attacker's own AWS account, zero CloudTrail in the target's environment. Great for lateral movement and short duration pivots, but I hit real operational limits during testing (12-hour lifetime, 1 Mbps ceiling, distinctive 20s keep-alive) that make it less ideal for persistent C2.

AWS IoT Core MQTT — Those Secure Tunneling limitations led me here. MQTT pub/sub with X.509 mTLS auth, no tunnel lifetime limits, indefinite persistence through *.iot.amazonaws.com. I built custom Mythic agents: Poseidon (Go) for Linux/macOS, Apollo (C#) for Windows, both validated on AMD64 and ARM64.

All the material will be available at the time of the presentation: Mythic agents and translation containers for both transports, infrastructure provisioning scripts, and detection rules (Suricata, Zeek, Splunk). Both Microsoft and AWS were engaged before disclosure. There's no vuln to patch, this is an architectural problem with how cloud relay services are designed.

SpeakerBio: Robert Pimentel, Hacker Hermanos

Robert is a seasoned offensive security professional with more than a decade of experience in Information Security.

He began his career in the U.S. Marine Corps, where he worked on secure telecommunications. Robert holds a master's degree in Cybersecurity, numerous IT certifications, and a background as an instructor at higher education institutions like the New Jersey Institute of Technology and American University.

Robert is committed to sharing his knowledge and experiences for the benefit of others. He enjoys Brazilian steakhouses and cuddling with his pugs while writing Infrastructure as Code to automate Red Team Infrastructure.

Robert is the Director of Offensive Security at Humana, Inc.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Minimal by Design: Building Hardened Near-Zero-CVE Container Images

Tags: Demo | Cloud Village | Creator Talk/Panel

When: Saturday, Aug 8, 13:00 - 13:30 PDT

Where: LVCCW Level 3 W313 (Cloud Village Talks) - [Map](#)

Description:

Most production containers ship on base images with dozens of known CVEs — debian:latest currently sits at 127. Patches take weeks. Your compliance team isn't happy. We built "minimal" — an open source project producing 36 hardened (and adding more), distroless container images for the stack most cloud teams actually run: Python, Node, Go, Redis, PostgreSQL, MySQL, Kafka, Nginx, Prometheus, Jenkins, and more. Image runs as non-root, has no shell, ships with a signed SBOM, and is rebuilt daily so CVE patches land in under 48 hours instead of 30 days. This talk is a practical walkthrough of how you build something like this from scratch using entirely open source tools — and what could go wrong. We'll cover the toolchain: Chainguard's melange for sandboxed source builds, apko for declarative image assembly, Wolfi as the package base, Grype for scanning, and cosign for keyless signing. We'll show the CI pipeline — 60 parallel GitHub Actions jobs, native ARM64 runners, ephemeral signing keys for PRs, multi-arch manifest assembly — and the 24 automated update workflows that track upstream releases daily across GitHub tags, RubyGems, php.net, and Wolfi's APKINDEX. We'll close with live Grype scan comparisons against official Docker Hub images. The numbers are dramatic, and they make the case better than we can. Every source build is SHA256-verified, and every assembled image is tested in CI before publishing — tests for no shell, correct entrypt, expected binaries present, services responding. Everything is open source and running in production today. If you leave this talk and build your own hardened container pipeline the next week, we've done our job.

Speakers: Kyle Quest, Ritvik Arya

SpeakerBio: Kyle Quest

Kyle is the creator of DockerSlim, a popular tool to secure and optimize containers. His area of focus is autonomous and secure cloud-native infrastructure, sandboxing and agent security. With over two decades in security, Kyle had a chance to wear many different hats as a builder, breaker, and defender. Currently reverse engineering coding agents like Claude Code for fun AND profit ;-)

SpeakerBio: Ritvik Arya

Ritvik Arya is an Application Security Engineer at Amazon Web Services specializing in cloud security, container security, and offensive security research. His work focuses on securing large-scale cloud-native applications, building hardened container ecosystems, and developing scalable AppSec automation and vulnerability discovery tooling.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Minimize Harm, Maximize Defense: How Anthropic Navigates the Offense-Defense Divide

Tags: AI Village | Creator Talk/Panel

When: Friday, Aug 7, 16:30 - 16:59 PDT

Where: LVCCW Level 1 Hall 3 1103 (Creator Stage 5) - [Map](#)

Description:

Cybersecurity capabilities are inherently dual use: the same tools that help defenders find and fix vulnerabilities can, in the wrong hands, be the precursor to a cyberattack. As AI models grow more capable, this tension intensifies. When Anthropic launched Claude Fable 5 with the strongest cybersecurity safeguards we have ever applied to a model, we were forced to make concrete decisions about where the line between defense and offense should be drawn.

In this talk, we walk through how we reason about that line. We describe the four categories our safety classifiers use to evaluate cybersecurity activity: prohibited use (high harm, little defensive utility), high-risk dual use (core security professional work that we block until better access controls exist), low-risk dual use (mostly defensive, but blocked as part of a deliberate safety margin), and benign use (defensive and IT activities we aim to never block). We explain the tradeoffs behind each category and why we deliberately set Fable 5's safety margin larger than any prior model, accepting a higher rate of false positives in exchange for greater confidence that harmful requests would be caught.

We also introduce an early version of the Cyber Jailbreak Severity (CJS) framework, which we continue to develop with our Glasswing partners to create a common industry standard for assessing how serious a given jailbreak is.

This is not a finished answer. These categories, thresholds, and tradeoffs represent our best current thinking, but we anticipate they will evolve as model capabilities advance, as the legal and regulatory landscape shifts, and as we learn from the security community's experience using these tools in practice. We are sharing our framework because the people most affected by where these lines are drawn should have a voice in drawing them.

SpeakerBio: Curt Barnard

No BIO available

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Aerospace Village - Friday - 10:00-17:59 PDT

Title: Mission: Compromised - Hacking a Satellite from the Ground Up

Tags: Aerospace Village | Creator Event/Activity

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 2 700 (Aerospace Village) - [Map](#)

Description:

Ever wondered what it takes to hack a satellite? At this hands-on station, you'll step into the role of an attacker targeting a CubeSat-class spacecraft and its ground control station — all running in a safe, fully isolated environment.

Working against a live mission control system (OpenC3 COSMOS / Yamcs) and a spacecraft simulator, you'll follow an attacker's kill chain across multiple layers — from reconnaissance and ground station compromise all the way to the spacecraft itself. Where does it end? Let's just say the mission doesn't survive. Come find out how. Every step is paired with the real-world defense that would have stopped it - so you'll leave understanding both how these attacks work and how space systems defend against them. Whether you're new to space security or already deep in the field, come try it out, break a satellite (safely!), and see the attack surface of modern spacecraft up close.

It will take approximately 15-30 minutes to work through this hands-on demo and guided exercises. You can watch attacks demonstrated by our team, then try guided scenarios yourself using real CCSDS space protocols, RF concepts, and industry mission control tooling. A live mission dashboard will reveal the spacecraft's fate as the scenario plays out.

No prior space experience required - all skill levels welcome. We recommend you bring your own laptop the hands-on portions. A laptop with GNU Radio will let you dig into the RF challenge, and a Kali Linux setup or your equivalent pentesting toolkit are recommended for the more advanced challenge.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Aerospace Village - Saturday - 10:00-17:59 PDT

Title: Mission: Compromised - Hacking a Satellite from the Ground Up

Tags: Aerospace Village | Creator Event/Activity

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 2 700 (Aerospace Village) - [Map](#)

Description:

Ever wondered what it takes to hack a satellite? At this hands-on station, you'll step into the role of an attacker targeting a CubeSat-class spacecraft and its ground control station — all running in a safe, fully isolated environment.

Working against a live mission control system (OpenC3 COSMOS / Yamcs) and a spacecraft simulator, you'll follow an attacker's kill chain across multiple layers — from reconnaissance and ground station compromise all the way to the spacecraft itself. Where does it end? Let's just say the mission doesn't survive. Come find out how. Every step is paired with the real-world defense that would have stopped it - so you'll leave understanding both how these attacks work and how space systems defend against them. Whether you're new to space security or already deep in the field, come try it out, break a satellite (safely!), and see the attack surface of modern spacecraft up close.

It will take approximately 15-30 minutes to work through this hands-on demo and guided exercises. You can watch attacks demonstrated by our team, then try guided scenarios yourself using real CCSDS space protocols, RF concepts, and industry mission control tooling. A live mission dashboard will reveal the spacecraft's fate as the scenario plays out.

No prior space experience required - all skill levels welcome. We recommend you bring your own laptop the hands-on portions. A laptop with GNU Radio will let you dig into the RF challenge, and a Kali Linux setup or your equivalent pentesting toolkit are recommended for the more advanced challenge.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Aerospace Village - Sunday - 10:00-13:59 PDT

Title: Mission: Compromised - Hacking a Satellite from the Ground Up

Tags: Aerospace Village | Creator Event/Activity

When: Sunday, Aug 9, 10:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 2 700 (Aerospace Village) - [Map](#)

Description:

Ever wondered what it takes to hack a satellite? At this hands-on station, you'll step into the role of an attacker targeting a CubeSat-class spacecraft and its ground control station — all running in a safe, fully isolated environment.

Working against a live mission control system (OpenC3 COSMOS / Yamcs) and a spacecraft simulator, you'll follow an attacker's kill chain across multiple layers — from reconnaissance and ground station compromise all the way to the spacecraft itself. Where does it end? Let's just say the mission doesn't survive. Come find out how. Every step is paired with the real-world defense that would have stopped it - so you'll leave understanding both how these attacks work and how space systems defend against them. Whether you're new to space security or already deep in the field, come try it out, break a satellite (safely!), and see the attack surface of modern spacecraft up close.

It will take approximately 15-30 minutes to work through this hands-on demo and guided exercises. You can watch attacks demonstrated by our team, then try guided scenarios yourself using real CCSDS space protocols, RF concepts, and industry mission control tooling. A live mission dashboard will reveal the spacecraft's fate as the scenario plays out.

No prior space experience required - all skill levels welcome. We recommend you bring your own laptop the hands-on portions. A laptop with GNU Radio will let you dig into the RF challenge, and a Kali Linux setup or your equivalent pentesting toolkit are recommended for the more advanced challenge.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Mobile Hacking Community - Friday - 10:00-17:59 PDT

Title: Mobile Hacking - Informal CTF

Tags: Mobile Hacking Community | Creator Event/Activity

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 4 1422 (Mobile Hacking Community) - [Map](#)

Description:

Capture the Flag (CTF) events featuring mobile application security challenges at varying levels of difficulty, also providing a ranking system to evaluate and compare participants' skills.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Mobile Hacking Community - Saturday - 10:00-17:59 PDT

Title: Mobile Hacking - Informal CTF

Tags: Mobile Hacking Community | Creator Event/Activity

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 4 1422 (Mobile Hacking Community) - [Map](#)

Description:

Capture the Flag (CTF) events featuring mobile application security challenges at varying levels of difficulty, also providing a ranking system to evaluate and compare participants' skills.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Mobile Hacking Community - Sunday - 10:00-11:59 PDT

Title: Mobile Hacking - Informal CTF

Tags: Mobile Hacking Community | Creator Event/Activity

When: Sunday, Aug 9, 10:00 - 11:59 PDT

Where: LVCCW Level 1 Hall 4 1422 (Mobile Hacking Community) - [Map](#)

Description:

Capture the Flag (CTF) events featuring mobile application security challenges at varying levels of difficulty, also providing a ranking system to evaluate and compare participants' skills.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Mobile Hacking Community - Open

Tags: Mobile Hacking Community | Creator Event/Activity

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 4 1422 (Mobile Hacking Community) - [Map](#)

Description:

At the Mobile Hacking Community, attendees will learn about the latest trends in mobile application security through hands-on experiences, including topics such as bypassing security mechanisms and hardening techniques, and exploiting known CVEs.

Additionally, attendees will engage in a competitive process by participating in an onsite CTF (Capture the Flag) event to test their skills, face new challenges, and learn new skills.

Attendees will also have the opportunity to watch cutting-edge research presentations and case studies on various topics within the domain.

Dedicated real devices running vulnerable applications will be available, allowing attendees to actively practice exploitation and analysis in a realistic environment.

Prerequisites:

- Attendees should bring their own laptop in order to fully participate in the hands-on workshops and CTF challenges.
- A basic familiarity with using a command line, installing software, and general computing concepts is recommended, but prior mobile security experience is not required.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Mobile Hacking Community - Open

Tags: Mobile Hacking Community | Creator Event/Activity

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 4 1422 (Mobile Hacking Community) - [Map](#)

Description:

At the Mobile Hacking Community, attendees will learn about the latest trends in mobile application security through hands-on experiences, including topics such as bypassing security mechanisms and hardening techniques, and exploiting known CVEs.

Additionally, attendees will engage in a competitive process by participating in an onsite CTF (Capture the Flag) event to test their skills, face new challenges, and learn new skills.

Attendees will also have the opportunity to watch cutting-edge research presentations and case studies on various topics within the domain.

Dedicated real devices running vulnerable applications will be available, allowing attendees to actively practice exploitation and analysis in a realistic environment.

Prerequisites:

- Attendees should bring their own laptop in order to fully participate in the hands-on workshops and CTF challenges.
- A basic familiarity with using a command line, installing software, and general computing concepts is recommended, but prior mobile security experience is not required.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Mobile Hacking Community - Open

Tags: Mobile Hacking Community | Creator Event/Activity

When: Sunday, Aug 9, 10:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 4 1422 (Mobile Hacking Community) - [Map](#)

Description:

At the Mobile Hacking Community, attendees will learn about the latest trends in mobile application security through hands-on experiences, including topics such as bypassing security mechanisms and hardening techniques, and exploiting known CVEs.

Additionally, attendees will engage in a competitive process by participating in an onsite CTF (Capture the Flag) event to test their skills, face new challenges, and learn new skills.

Attendees will also have the opportunity to watch cutting-edge research presentations and case studies on various topics within the domain.

Dedicated real devices running vulnerable applications will be available, allowing attendees to actively practice exploitation and analysis in a realistic environment.

Prerequisites:

- Attendees should bring their own laptop in order to fully participate in the hands-on workshops and CTF challenges.
- A basic familiarity with using a command line, installing software, and general computing concepts is recommended, but prior mobile security experience is not required.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

The Diana Initiative - Friday - 11:20-11:30 PDT

Title: Mobile Hacking Tour

Tags: The Diana Initiative | Creator Tour

When: Friday, Aug 7, 11:20 - 11:30 PDT

Where: LVCCW Level 1 South Lobby / Atrium - [Map](#)

Description:

Interested in visiting Mobile Hacking but afraid to go by yourself? The Diana Initiative is hosting tours! Follow a volunteer to Mobile Hacking and be introduced to the community and activities inside!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Mobile Hacking Community - Friday - 15:00-15:45 PDT

Title: Mobile Security through Obscurity, from insecure client-side encryption to unauthenticated SQL

Tags: Mobile Hacking Community | Creator Talk/Panel

When: Friday, Aug 7, 15:00 - 15:45 PDT

Where: LVCCW Level 1 Hall 4 1422 (Mobile Hacking Community) - [Map](#)

Description:

In this talk the Just Mobile Security team will talk about the Mobile Security through Obscurity, from insecure client-side encryption to unauthenticated SQLi. Talking about a lot of LATAM Banks and Fintechs who implemented that in their applications.

Speakers: Juan Urbano Stordeur, Juan Martinez Blanco

SpeakerBio: Juan Urbano Stordeur, CEO and Founder at Just Mobile Security

No BIO available

SpeakerBio: Juan Martinez Blanco, Mobile Security Penetration Tester at Just Mobile Security

No BIO available

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Monitor, Compile, Enforce: A Compiler Pipeline for Container Security Policy in Rust and eBPF

Tags: DEF CON Demo Labs | Advanced | Cloud | Defense/Blue Team | DEF CON Demo Labs

When: Saturday, Aug 8, 10:00 - 10:45 PDT

Where: LVCCW Level 1 Hall 3 902 (Demo Labs Track 6) - [Map](#)

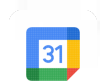
Description:

Container security tools observe behavior (eBPF) and enforce policy (BPF-LSM, AppArmor, Seccomp). But the translation between observation and enforcement is manual and incomplete. We present the first tool that treats this translation as a compilation problem. Built in Rust with the Aya eBPF framework, three monitoring modules serve as compiler frontends feeding a normalized behavioral IR. Optimization passes operate on this IR: pattern classification, rule deduplication, dead rule elimination, conflict detection, and cross-category dependency linking. The backend compiles optimized IR into BPF-LSM enforcement rules across three LSM hooks: `security_file_open`, `security_bprm_check_security`, and `security_socket_connect`. Enforcement is default-deny: any operation not in the compiled profile is blocked. We demo end-to-end: a container is profiled, the profile compiled through the pipeline, and enforcement blocks unauthorized file access, process execution, and network connections at the kernel level. Zero manual policy writing. We document the friction points where monitoring context diverges from enforcement context. No existing tool, including vArmor and KubeArmor, implements this compilation architecture with a true IR, optimization passes, and multi-category LSM enforcement.

SpeakerBio: Buğrahan Yücel

Buğrahan Yücel is a software engineer at a SaaS company in Turkey, where he works on infrastructure security. He currently builds eBPF-based behavioral profiling and enforcement tooling in Rust using the Aya framework. This is his first DEF CON presentation.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Monitor, Compile, Enforce: A Compiler Pipeline for Container Security Policy in Rust and eBPF

Tags: DEF CON Demo Labs | Advanced | Cloud | Defense/Blue Team | DEF CON Demo Labs

When: Friday, Aug 7, 13:00 - 13:45 PDT

Where: LVCCW Level 1 Hall 3 902 (Demo Labs Track 6) - [Map](#)

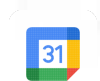
Description:

Container security tools observe behavior (eBPF) and enforce policy (BPF-LSM, AppArmor, Seccomp). But the translation between observation and enforcement is manual and incomplete. We present the first tool that treats this translation as a compilation problem. Built in Rust with the Aya eBPF framework, three monitoring modules serve as compiler frontends feeding a normalized behavioral IR. Optimization passes operate on this IR: pattern classification, rule deduplication, dead rule elimination, conflict detection, and cross-category dependency linking. The backend compiles optimized IR into BPF-LSM enforcement rules across three LSM hooks: `security_file_open`, `security_bprm_check_security`, and `security_socket_connect`. Enforcement is default-deny: any operation not in the compiled profile is blocked. We demo end-to-end: a container is profiled, the profile compiled through the pipeline, and enforcement blocks unauthorized file access, process execution, and network connections at the kernel level. Zero manual policy writing. We document the friction points where monitoring context diverges from enforcement context. No existing tool, including vArmor and KubeArmor, implements this compilation architecture with a true IR, optimization passes, and multi-category LSM enforcement.

SpeakerBio: Buğrahan Yücel

Buğrahan Yücel is a software engineer at a SaaS company in Turkey, where he works on infrastructure security. He currently builds eBPF-based behavioral profiling and enforcement tooling in Rust using the Aya framework. This is his first DEF CON presentation.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Blacks In Cyber Village - Sunday - 12:00-12:20 PDT

Title: Monocultures Are Vulnerabilities: Representation and Security in STEM

Tags: Blacks In Cyber Village | Creator Talk/Panel

When: Sunday, Aug 9, 12:00 - 12:20 PDT

Where: LVCCW Level 3 W322-W324 (BIC Village) - [Map](#)

Description:

This thought-provoking session argues that equity and representation in STEM are essential security controls, not just optional add-ons. Discover how monocultures create vulnerabilities in cybersecurity and technology by fostering blind spots to critical threats. Learn how diverse perspectives act as an inoculation, strengthening our collective ability to anticipate and resist both human and algorithmic abuses. This talk highlights why inclusive pipelines are fundamental for building more secure and resilient systems for all.

SpeakerBio: Ruben Stephen, Undergraduate Student, MIT

Ruben Stephen is an MIT student pursuing dual majors in Mechanical Engineering and Computer Science. Driven by a passion for problem-solving, personal growth, and helping others, they also embrace digital creation and entrepreneurship to amplify their impact and explore their love of system building from a different lens.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Morbidity and Mortality: Hackers, HIPAA, and a new Prescription for Healthcare Cyber Policy

Tags: Policy @ DEF CON | Creator Talk/Panel

When: Friday, Aug 7, 11:00 - 11:59 PDT

Where: LVCCW Level 2 W210-211 (Policy Village) - [Map](#)

Description:

US healthcare cybersecurity policy has flatlined. An eruption of targeted ransomware is only the latest epidemic plaguing a beleaguered sector facing workforce shortages, grappling with legacy medical devices and dependent on a complex web of vulnerable third party vendors. As patients suffer, doctors and nurses struggle, and hospitals bleed money they don't have, critical public health stakeholders and institutions are failing to meet the moment. How did we get here? Join quaddi & r3plicant, two physician hackers and amateur wonks as they take you through a cyber policy autopsy - diagnosing the decisions and dilemmas that have resulted in this current crisis. From a diseased culture of secrecy predicated on a willful misunderstanding of privacy regulation to outdated national response and recovery frameworks, this talk will explore how policy choices made at the dawn of medicine's digitization have aged poorly in an era of health system consolidation, single point of failure dependencies, and a rabid push to integrate AI into everything from thermometers to transplant surgery. The prognosis isn't all dire. From a revitalized HIPAA to bipartisan bills to resuscitate rural hospitals, a policy prescription exists to better protect patients and secure systems. It's time to take your medicine.

Speakers: Christian Dameff, Jeff "r3plicant" Tully

SpeakerBio: Christian Dameff, UC San Diego Center for Healthcare Cybersecurity

Christian (quaddi) Dameff, MD is an ER doc and Associate Professor of Emergency Medicine, Biomedical Informatics, and Computer Science (Affiliate) at the University of California San Diego, where he also co-directs the Center for Healthcare Cybersecurity. He is a hacker, former open capture the flag champion, and prior DEF CON/RSA/Blackhat/HIMSS Speaker. He previously has testified in front of the U.S. Congress and U.S. Food and Drug Administration.

SpeakerBio: Jeff "r3plicant" Tully, UC San Diego Center for Healthcare Cybersecurity

Jeff (r3plicant) Tully, MD is a security researcher with an interest in understanding the ever-growing intersections between healthcare and technology. His research has been highlighted in international media, leading academic medical journals and cease and desist letters sent on behalf of billion-dollar cybersecurity corporations. As an elected member of the Health Sector Coordinating Council Cyber Working Group's Executive Committee he regularly engages with policymakers and other federal healthcare cybersecurity stakeholders. During his day job as an anesthesiologist, he focuses primarily on the delivery of oxygen to tissues.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Most threat modeling artifacts don't help coding agents fix business logic. Here's what does.

Tags: AppSec Village | Creator Talk/Panel | All Audiences

When: Friday, Aug 7, 16:50 - 17:20 PDT

Where: LVCCW Level 1 Hall 2 604 (Appsec Village) Main Stage - [Map](#)

Description:

Coding agents increasingly produce code that looks clean to static analysis, but still ship business-logic bugs: the kind threat modeling is supposed to prevent. Across 86 controlled experiments, we varied the security context given to gpt-5.5-codex across eight artifact families and three prompt structures, using the same codebase, PRD, and four planted business-logic flaws. Generic artifacts - DFDs, component diagrams, OWASP checklists - did not reliably help; several performed worse than no artifact at all. In one run, the agent - handed an OWASP checklist - cited A07 in its plan and shipped a 365-day bookmarkable magic link, the exact vulnerability A07 names. One pattern worked across every replication: feature-specific threats paired with concrete countermeasures, in a plan-forcing prompt. The talk walks through the mechanism behind these failure modes and the open-source tool we built to generate the artifact shape that worked.

SpeakerBio: Meitar Ronen

Meitar Ronen is AI Research Lead at Clover Security, where she drives the research direction for agentic development and AI infrastructure. She previously built computer vision algorithms and holds an M.Sc. in computer science with a focus on deep learning, with publications at CVPR and ICCV. She turned to the dark side and now leads AI research for cyber, focused on the hard problems that decide whether security agents can be trusted with real work.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Aerospace Village - Friday - 10:00-17:59 PDT

Title: MOUSE Runner & Flappy Drone

Tags: Aerospace Village | Creator Event/Activity

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 2 700 (Aerospace Village) - [Map](#)

Description:

How High Can You Make a Satellite Jump? Can You Fly a Drone Around Aliens and Rockets?

Put your action-hero reflexes and hand-eye coordination to the test as you battle fellow DEF CON attendees for the top scores in MOUSE Runner and Flappy Drone. The highest scores on Friday and Saturday will earn a special prize. Stop by our booth to learn more, show off your button-mashing skills, and prove you're the ultimate space cyber pilot.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Aerospace Village - Saturday - 10:00-17:59 PDT

Title: MOUSE Runner & Flappy Drone

Tags: Aerospace Village | Creator Event/Activity

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 2 700 (Aerospace Village) - [Map](#)

Description:

How High Can You Make a Satellite Jump? Can You Fly a Drone Around Aliens and Rockets?

Put your action-hero reflexes and hand-eye coordination to the test as you battle fellow DEF CON attendees for the top scores in MOUSE Runner and Flappy Drone. The highest scores on Friday and Saturday will earn a special prize. Stop by our booth to learn more, show off your button-mashing skills, and prove you're the ultimate space cyber pilot.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Aerospace Village - Sunday - 10:00-13:59 PDT

Title: MOUSE Runner & Flappy Drone

Tags: Aerospace Village | Creator Event/Activity

When: Sunday, Aug 9, 10:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 2 700 (Aerospace Village) - [Map](#)

Description:

How High Can You Make a Satellite Jump? Can You Fly a Drone Around Aliens and Rockets?

Put your action-hero reflexes and hand-eye coordination to the test as you battle fellow DEF CON attendees for the top scores in MOUSE Runner and Flappy Drone. The highest scores on Friday and Saturday will earn a special prize. Stop by our booth to learn more, show off your button-mashing skills, and prove you're the ultimate space cyber pilot.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Social Gatherings/Events - Saturday - 20:00-23:59 PDT

Title: Movie Night

Tags: Event

When: Saturday, Aug 8, 20:00 - 23:59 PDT

Where: LVCCW Level 2 W225 (Workshops) - [Map](#)

Description:



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Social Gatherings/Events - Friday - 20:00-23:59 PDT

Title: Movie Night

Tags: Event

When: Friday, Aug 7, 20:00 - 23:59 PDT

Where: LVCCW Level 2 W225 (Workshops) - [Map](#)

Description:



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: MSCodePhish: Redeem Your Coupon. Surrender Your Session

Tags: Intro/Beginner | DEF CON Demo Labs | Cloud | Offense/Red Team | DEF CON Demo Labs

When: Friday, Aug 7, 13:00 - 13:45 PDT

Where: LVCCW Level 1 Hall 3 1002 (Demo Labs Track 2) - [Map](#)

Description:

MSCodePhish is a red team toolkit that turns Microsoft's Device Code OAuth flow into an embeddable phishing primitive that works inside any lure (e.g., "grab your coupon," "unlock access," etc.). Instead of pre-generating device codes and racing against the usual 15 minute timeout, MSCodePhish exposes a simple API endpoint that phishing pages can call via JavaScript (XHR/fetch) at the exact moment a victim opens the page. The tool then generates a fresh device code on demand, returns it to the phishing page (e.g., rendered as a "coupon code"), and instructs the user to complete the login on the legitimate Microsoft device login portal using that code.

Behind the scenes, MSCodePhish continuously polls Microsoft's token endpoint for that device code and, once the victim finishes authentication, captures the resulting refresh token and related claims (tenant, user, etc.). From its web UI, operators can track active campaigns, monitor which lures are converting, and use captured refresh tokens to request new access tokens for different resources (ARM, Key Vault, Graph, Storage, or custom scopes) in real time. Because the code is generated only when the phishing HTML is actually loaded, MSCodePhish effectively sidesteps device code expiration issues and enables more realistic, flexible phishing flows that closely mimic

Speakers: Raunak "Trouble1" Parmar, Chirag "3xpl01tc0d3r" Savla

SpeakerBio: Raunak "Trouble1" Parmar

Raunak Parmar works as a senior cloud security engineer at White Knight Labs with 6+ years of experience. His areas of interest include web penetration testing, Azure/AWS security, source code review, scripting, and development. He enjoys researching new attack methodologies and creating open-source tools that can be used during cloud red team activities. He has worked extensively on Azure and AWS and is the author of Vajra, AzDevRecon and MsCodePhish. He has spoken at multiple respected security conferences like Black Hat, Defcon, Nullcon, RootCon, HackspaceCon, NorthSec, LeHack, etc and also at local meetups.

SpeakerBio: Chirag "3xpl01tc0d3r" Savla

Chirag Savla is a Cyber Security professional with 10+ years of experience. His areas of interest include penetration testing, red teaming, azure and active directory security, and post-exploitation research. He prefers to create open-source tools and explore new attack methodologies in his leisure. He has worked extensively on Azure, Active Directory attacks, defense, and bypassing detection mechanisms. He is an author of multiple Open Source tools such as Process Injection, Callidus, etc. He has presented at multiple conferences and local meetups and has trained people in international conferences like Blackhat, BSides Milano, Wild West Hackin, etc.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: MSCodePhish: Redeem Your Coupon. Surrender Your Session

Tags: Intro/Beginner | DEF CON Demo Labs | Cloud | Offense/Red Team | DEF CON Demo Labs

When: Saturday, Aug 8, 12:00 - 12:45 PDT

Where: LVCCW Level 1 Hall 3 1002 (Demo Labs Track 2) - [Map](#)

Description:

MSCodePhish is a red team toolkit that turns Microsoft's Device Code OAuth flow into an embeddable phishing primitive that works inside any lure (e.g., "grab your coupon," "unlock access," etc.). Instead of pre-generating device codes and racing against the usual 15 minute timeout, MSCodePhish exposes a simple API endpoint that phishing pages can call via JavaScript (XHR/fetch) at the exact moment a victim opens the page. The tool then generates a fresh device code on demand, returns it to the phishing page (e.g., rendered as a "coupon code"), and instructs the user to complete the login on the legitimate Microsoft device login portal using that code.

Behind the scenes, MSCodePhish continuously polls Microsoft's token endpoint for that device code and, once the victim finishes authentication, captures the resulting refresh token and related claims (tenant, user, etc.). From its web UI, operators can track active campaigns, monitor which lures are converting, and use captured refresh tokens to request new access tokens for different resources (ARM, Key Vault, Graph, Storage, or custom scopes) in real time. Because the code is generated only when the phishing HTML is actually loaded, MSCodePhish effectively sidesteps device code expiration issues and enables more realistic, flexible phishing flows that closely mimic

Speakers: Raunak "Trouble1" Parmar, Chirag "3xpl01tc0d3r" Savla

SpeakerBio: Raunak "Trouble1" Parmar

Raunak Parmar works as a senior cloud security engineer at White Knight Labs with 6+ years of experience. His areas of interest include web penetration testing, Azure/AWS security, source code review, scripting, and development. He enjoys researching new attack methodologies and creating open-source tools that can be used during cloud red team activities. He has worked extensively on Azure and AWS and is the author of Vajra, AzDevRecon and MsCodePhish. He has spoken at multiple respected security conferences like Black Hat, Defcon, Nullcon, RootCon, HackspaceCon, NorthSec, LeHack, etc and also at local meetups.

SpeakerBio: Chirag "3xpl01tc0d3r" Savla

Chirag Savla is a Cyber Security professional with 10+ years of experience. His areas of interest include penetration testing, red teaming, azure and active directory security, and post-exploitation research. He prefers to create open-source tools and explore new attack methodologies in his leisure. He has worked extensively on Azure, Active Directory attacks, defense, and bypassing detection mechanisms. He is an author of multiple Open Source tools such as Process Injection, Callidus, etc. He has presented at multiple conferences and local meetups and has trained people in international conferences like Blackhat, BSides Milano, Wild West Hackin, & Fest.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: MSIX'd Up: Weaponizing the Modern Windows App Packaging Ecosystem

Tags: DEF CON Official Talk | Demo | Tool | Exploit

When: Sunday, Aug 9, 12:00 - 12:59 PDT

Where: LVCCW Level 1 Hall 3 1007 (Main Track 2) - [Map](#)

Description:

What happens when the ecosystem Microsoft built for isolation and integrity of modern Windows applications becomes a foundation for novel attacker tradecraft?

For over 13 years, an ecosystem that now includes MSIX, UWP, AppContainers, package identity, and the Windows Runtime has shipped by default on modern Windows. Yet offensive research into this ecosystem remains scarce, and visibility into its abuse lags further behind. In this talk, we demonstrate novel techniques spanning all major parts of an attack path.

For initial access, we abuse URL protocol handlers and packaging file formats to subvert endpoint detections. For post-exploitation, we overcome AppContainer process isolation to operate beneath EDR visibility thresholds. For lateral movement, we expose previously unabused WMI providers and DCOM objects within package installation services. For privilege escalation, we chain a logic flaw in package capabilities to achieve SYSTEM from a standard user context. Every technique requires no third-party software, works on fully patched systems, and abuses default-enabled features. Tools for red teams will be released alongside detection guidance for defenders.

The modern app packaging ecosystem was designed for isolation and integrity. We used its design to our advantage and turned it into an attack platform.

<https://projectzero.google/2021/08/understanding-network-access-windows-app.html>

<https://www.pentestpartners.com/security-blog/ms-enterprise-app-management-service-rce-cve-2022-35841/>

[https://conference.hitb.org/hitbsecconf2018pek/materials/D1T2%20-%20The%20Inner%20Workings%20of%20the%20Windows%](https://conference.hitb.org/hitbsecconf2018pek/materials/D1T2%20-%20The%20Inner%20Workings%20of%20the%20Windows%20App%20Packaging%20Ecosystem.pdf)

<https://activecyber.us/activelabs/windows-appx-deployment-service-local-privilege-escalation-cve-2020-1488>

SpeakerBio: Nick "zyn3rgy" Powers, SpecterOps

An offensive security professional with experience in leading and offering red team assessments and penetration testing across several attack surfaces to a diverse set of industries. Professional interests include furthering knowledge of Windows internals, static and dynamic Endpoint Detection & Response (EDR) evasion, as well as initial access attack surface research. Passionate about contributing back to the security community by speaking at conferences such as Defcon, Wild West Hackin' Fest, and Troopers along with instructing course content at conferences such as BlackHat USA.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Social Gatherings/Events - Thursday - 21:00-21:59 PDT

Title: Music - Genre: Breakbeats

Tags: Entertainment

When: Thursday, Aug 6, 21:00 - 21:59 PDT

Where: LVCCW Level 1 W107-W109 (Chillout Lounge) - [Map](#)

Description:

SpeakerBio: PatAttack

PatAttack is a Seattle Based DJ who loves EDM. He is a Security Nerd who hunts logs by day and plays beats by night.



[Return to Index](#) - Add to Google

- ics [Calendar](#) file

Social Gatherings/Events - Thursday - 22:00-22:59 PDT

Title: Music - Genre: Breakbeats

Tags: Entertainment

When: Thursday, Aug 6, 22:00 - 22:59 PDT

Where: LVCCW Level 1 W107-W109 (Chillout Lounge) - [Map](#)

Description:

SpeakerBio: Icetre Normal

Forever lurking the hallowed halls of records, tapes, 8-Tracks, Icetre has been bringing the best in breakbeats, jungle, drum and bass, electro, house, goth, industrial, found sounds, and oddball records to craft the tightest, freshest and oddest music in the hacker scene.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Social Gatherings/Events - Saturday - 20:00-20:59 PDT

Title: Music - Genre: Drum & Bass

Tags: Entertainment

When: Saturday, Aug 8, 20:00 - 20:59 PDT

Where: LVCCW Level 1 W107-W109 (Chillout Lounge) - [Map](#)

Description:

SpeakerBio: RELAY

With over 25 years of experience, RELAY is fluent in the language of electronic music, effortlessly blending genres ranging from house, trance and techno to bass music, electro and drum and bass while also incorporating turntablism. His sets promise to keep the vibe alive.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Social Gatherings/Events - Saturday - 22:00-22:59 PDT

Title: Music - Genre: Drum & Bass

Tags: Entertainment

When: Saturday, Aug 8, 22:00 - 22:59 PDT

Where: LVCCW Level 1 W107-W109 (Chillout Lounge) - [Map](#)

Description:

SpeakerBio: Miss Jackalope

Miss Jackalope is DEF CON's Resident DJ. She's played all sorts of awesome events, parties, and infosec conventions. Her current faves are drum and bass and electro. Usually she is spotted getting abused by her cat while trying to spin on her weekly Twitch show (twitch.tv/missjackalope) and in the DC Vendor room selling her legendary merch. She is the DEF CON Arts and Entertainment evangelist and leader of the Mighty Jackalope Army. She also has a massive pile of claw game fun and Twitch replays on her Youtube channel! (youtube.com/@MissJackalope) Come join the party!

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Social Gatherings/Events - Saturday - 23:00-23:59 PDT

Title: Music - Genre: Drum & Bass

Tags: Entertainment

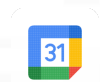
When: Saturday, Aug 8, 23:00 - 23:59 PDT

Where: LVCCW Level 1 W107-W109 (Chillout Lounge) - [Map](#)

Description:

SpeakerBio: Syntax + Luna

Syntax has been DJing almost as long as he's been hacking, experienced in a variety of genres and currently obsessed with Drum & Bass. Luna started joining Syntax on stage in the last few years by mixing their visuals with the same live intensity. Together they perform at hacker cons across the US—plus other shows in between—always blasting earholes and bouncing eyeballs to the best bass-y beats.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Social Gatherings/Events - Sunday - 00:00-00:59 PDT

Title: Music - Genre: Drum & Bass

Tags: Entertainment

When: Sunday, Aug 9, 00:00 - 00:59 PDT

Where: LVCCW Level 1 W107-W109 (Chillout Lounge) - [Map](#)

Description:

SpeakerBio: DJ XORAC

I like hacking and music :)

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Social Gatherings/Events - Saturday - 19:00-19:59 PDT

Title: Music - Genre: Dubstep

Tags: Entertainment

When: Saturday, Aug 8, 19:00 - 19:59 PDT

Where: LVCCW Level 1 W107-W109 (Chillout Lounge) - [Map](#)

Description:

SpeakerBio: ZipZapZop

Clark ov Saturn, Space Trucking Mogul, aka ZipZapZop has been releasing music off and on since the late 1980's. Notable projects have included pH10 (Terraformat Records, Europe tour with Trumystic Sound System 1999), Socks and Sandals (Microcosm Music, Unfoundsound Records) and resident DJ at Halcyon's weekly Deep Unda Brooklyn Undercity party in NYC in the early 2000's. After a long break focusing on family, an educational technology career and earning a doctorate, Saturn returned to music production with several projects since 2021: ZipZapZop, Pill Hill Deans, Luther VanGross and DubRatz, each featuring a variety of sounds, sub pressure bass-oriented music styles and friends, with the goals of fun, travel and liberation via creativity. More info, videos, links & connections at ZipZapZop.com

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Social Gatherings/Events - Thursday - 20:00-20:59 PDT

Title: Music - Genre: Electro House

Tags: Entertainment

When: Thursday, Aug 6, 20:00 - 20:59 PDT

Where: LVCCW Level 1 W107-W109 (Chillout Lounge) - [Map](#)

Description:

SpeakerBio: Archwisp

Resident DCP beatsmaker



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Social Gatherings/Events - Friday - 19:00-19:59 PDT

Title: Music - Genre: Goth / Industrial

Tags: Entertainment

When: Friday, Aug 7, 19:00 - 19:59 PDT

Where: LVCCW Level 1 W107-W109 (Chillout Lounge) - [Map](#)

Description:

SpeakerBio: Daemon Chadeau

From the darkest lit nightclubs to the livestreaming virtual nightlife, DJ Daemon Chadeau has imposed their will upon sound systems and dance floors all over the US since 2003. A native of Southern California, Daemon has been a staple of Seattle's Mercury at Machineworks since moving to the Northwest in 2011 and has been highlighting the bleeding edge in music from all around the diaspora of dark music, whether it is harsh industrial, power noise, darkwave, or bass-saturated electronic beats, and everything in between. After being recognized by their peers in both 2014 and 2015 as the Best Local Industrial DJ at the Mechanismus Industrial Music Awards, Daemon expanded beyond their home base and has performed at venues such as The Coffin Club (PDX), The Church Nightclub (DEN), and QXT's (NJ), as well as larger events such as Convergence XXI (LA), The Mechanismus Festival (2022 & 2025), The 2026 Seattle Fetish Ball, The Arcane Vampire Ball (DEN), and the main stage at DEFCONs 32 & 33 (LV). You can catch Daemon at The Mercury on 2nd Wednesdays (Protokol) and 3rd Fridays (Tech Noir), as well as at Time Warp for Continuum every 2nd Thursday! Outside of the decks, Daemon is the bassist for Seattle-area rock band Prelude To A Pistol, and is also the producer/composer/evil kitty mastermind Sir Kitty Meow-Meow in the experimental meower noise project Pixelpussy. Daemon has also been heavily involved with community engagement in the Seattle area, from mentoring up-and-coming DJs to having served as President of Gothic Pride Seattle from 2021 to 2024.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Social Gatherings/Events - Friday - 20:00-20:59 PDT

Title: Music - Genre: Goth / Industrial

Tags: Entertainment

When: Friday, Aug 7, 20:00 - 20:59 PDT

Where: LVCCW Level 1 W107-W109 (Chillout Lounge) - [Map](#)

Description:

SpeakerBio: DJ Scythe

SoCal/Vegas-based DJ Scythe spins Industrial/Aggrotech/Witch House/Synthpop/Synthwave/EBM/EBSM and all manners of dark and heavy music. He is a founding member and resident DJ of UnterKlub, Club Fallout, GothCon, and Nachturnal, Resident DJ at AREA15, and previously of BatCave LA. He regularly DJs the main stages for DEFCON, Wasteland Weekend and Neotropolis, and has done headlining shows for Torture Garden, Bondage Ball, Das Bunker, and others. Also a producer, his music can be found as SCYTHE, Artifact Corruption, and various other projects and is honored to have had his music featured on the Official DefCon 28 Safe Mode tape and various releases since.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Social Gatherings/Events - Friday - 22:00-22:59 PDT

Title: Music - Genre: House

Tags: Entertainment

When: Friday, Aug 7, 22:00 - 22:59 PDT

Where: LVCCW Level 1 W107-W109 (Chillout Lounge) - [Map](#)

Description:

SpeakerBio: Skittish & Bus

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Social Gatherings/Events - Thursday - 19:00-19:59 PDT

Title: Music - Genre: House

Tags: Entertainment

When: Thursday, Aug 6, 19:00 - 19:59 PDT

Where: LVCCW Level 1 W107-W109 (Chillout Lounge) - [Map](#)

Description:

SpeakerBio: matrix

matrix is a DJ in the Los Angeles area. He started DJing at hacker events such as Toorcon, ShellCon and DEFCON. matrix has DJ'd at the Linq Pool and other night clubs and bars. matrix prefers Tech House and Open Format DJ genres but can perform within a wide range of genres.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Social Gatherings/Events - Friday - 21:00-21:59 PDT

Title: Music - Genre: Nerdcore

Tags: Entertainment

When: Friday, Aug 7, 21:00 - 21:59 PDT

Where: LVCCW Level 1 W107-W109 (Chillout Lounge) - [Map](#)

Description:

SpeakerBio: Ohm-I

Ohm-I is a nerdcore rapper, saxophonist, and red teamer who mixes humor, storytelling, and a hacker perspective into clever and fun #BARS.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Social Gatherings/Events - Saturday - 21:00-21:59 PDT

Title: Music - Genre: Nerdcore

Tags: Entertainment

When: Saturday, Aug 8, 21:00 - 21:59 PDT

Where: LVCCW Level 1 W107-W109 (Chillout Lounge) - [Map](#)

Description:

SpeakerBio: Dual Core

Dual Core is an international hip hop duo. Drink all the booze; hack all the things!



[Return to Index](#) - Add to Google

- ics [Calendar](#) file

Social Gatherings/Events - Friday - 00:00-00:59 PDT

Title: Music - Genre: Techno

Tags: Entertainment

When: Friday, Aug 7, 00:00 - 00:59 PDT

Where: LVCCW Level 1 W107-W109 (Chillout Lounge) - [Map](#)

Description:

SpeakerBio: dotornot

With his trusty decks and mixer, DotOrNot unleashes a barrage of electrifying beats, showcasing the full spectrum of electronic music, from techno to house & DnB. DotOrNot is a champion of the underground, a protector of the genre, and a hero to all who dance to the beat of his music.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Social Gatherings/Events - Thursday - 23:00-23:59 PDT

Title: Music - Genre: Techno

Tags: Entertainment

When: Thursday, Aug 6, 23:00 - 23:59 PDT

Where: LVCCW Level 1 W107-W109 (Chillout Lounge) - [Map](#)

Description:

SpeakerBio: Scotch and Bubbles

“Scotch and Bubbles” is Zack “is it whiskey or whisky?” Fasel (@zfasel) and Erin “it’s not Champagne if it’s not from Champagne!” Jacobs (@secbarbie). Their history of bringing the untz, unce, and wubz to underground cyberdomes, ransomware recovery meetings, and 4 hour tarmac flight delays has put them on the global map, with performances stretching from Berlin to Bangkok. Bringing a mix of progressive, electro, future bass, and house, the duo has toured the world playing at events such as DEF CON, Shmoocon, Holy Sailboat, indoor cycling centers for the elderly, and as reenact-ors on America’s Most Wanted – Cyber Edition.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Social Gatherings/Events - Friday - 23:00-23:59 PDT

Title: Music - Genre: Techno

Tags: Entertainment

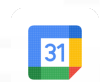
When: Friday, Aug 7, 23:00 - 23:59 PDT

Where: LVCCW Level 1 W107-W109 (Chillout Lounge) - [Map](#)

Description:

SpeakerBio: TRIODE

For up-and-coming uplifting trance DJ/Producer based out of San Francisco, Triode, music is much more than words could ever explain. Music serves as the cinematic backdrop to each of our stories, and as a DJ he sees it as his job to curate the perfect soundtrack to celebrate this amazing thing we call 'life'. Whether it's on the dancefloor, or in the studio producing his own beats - Triode's takes his listeners for a ride, into a magical place where you become the hero of this musical journey.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Social Gatherings/Events - Saturday - 00:00-00:59 PDT

Title: Music - Genre: Trance

Tags: Entertainment

When: Saturday, Aug 8, 00:00 - 00:59 PDT

Where: LVCCW Level 1 W107-W109 (Chillout Lounge) - [Map](#)

Description:

SpeakerBio: ~ -

AfterGlow is a Los Angeles-based DJ known for his electrifying sets that span across a wide range of EDM genres. Captivating crowds with his high-energy performances and infectious beats. Whether performing at intimate venues, events, or clubs, his sets leave a lasting impression that are sure to make you a fan.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Social Gatherings/Events - Saturday - 10:00-18:59 PDT

Title: Music - SomaFM

Tags: Entertainment

When: Saturday, Aug 8, 10:00 - 18:59 PDT

Where: LVCCW Level 1 W107-W109 (Chillout Lounge) - [Map](#)

Description:

SomaFM is back in the Chillout Lounge— just off the atrium at the south entrance (W107-W109). SomaFM DJs including kampf, Rusty, Merin MC, djdead and special guests will provide the perfect soundtrack for hacking or relaxing. Stop by and say hello, and pick up a 2026 limited edition sticker. We'll also be broadcasting live on <https://somafm.com/live/> – And did we mention, we have stickers!?



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Social Gatherings/Events - Thursday - 10:00-18:59 PDT

Title: Music - SomaFM

Tags: Entertainment

When: Thursday, Aug 6, 10:00 - 18:59 PDT

Where: LVCCW Level 1 W107-W109 (Chillout Lounge) - [Map](#)

Description:

SomaFM is back in the Chillout Lounge— just off the atrium at the south entrance (W107-W109). SomaFM DJs including kampf, Rusty, Merin MC, djdead and special guests will provide the perfect soundtrack for hacking or relaxing. Stop by and say hello, and pick up a 2026 limited edition sticker. We'll also be broadcasting live on <https://somafm.com/live/> – And did we mention, we have stickers!?



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Social Gatherings/Events - Friday - 10:00-18:59 PDT

Title: Music - SomaFM

Tags: Entertainment

When: Friday, Aug 7, 10:00 - 18:59 PDT

Where: LVCCW Level 1 W107-W109 (Chillout Lounge) - [Map](#)

Description:

SomaFM is back in the Chillout Lounge— just off the atrium at the south entrance (W107-W109). SomaFM DJs including kampf, Rusty, Merin MC, djdead and special guests will provide the perfect soundtrack for hacking or relaxing. Stop by and say hello, and pick up a 2026 limited edition sticker. We'll also be broadcasting live on <https://somafm.com/live/> – And did we mention, we have stickers!?



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Social Gatherings/Events - Sunday - 10:00-14:59 PDT

Title: Music - SomaFM

Tags: Entertainment

When: Sunday, Aug 9, 10:00 - 14:59 PDT

Where: LVCCW Level 1 W107-W109 (Chillout Lounge) - [Map](#)

Description:

SomaFM is back in the Chillout Lounge— just off the atrium at the south entrance (W107-W109). SomaFM DJs including kampf, Rusty, Merin MC, djdead and special guests will provide the perfect soundtrack for hacking or relaxing. Stop by and say hello, and pick up a 2026 limited edition sticker. We'll also be broadcasting live on <https://somafm.com/live/> – And did we mention, we have stickers!?



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Telecom Village - Friday - 16:00-16:30 PDT

Title: Nation State Obfuscation Networks

Tags: Telecom Village | Creator Talk/Panel

When: Friday, Aug 7, 16:00 - 16:30 PDT

Where: LVCCW Level 3 W321 (Telecom Village) - [Map](#)

Description:

1. Edge devices are now the primary obfuscation layer for state-sponsored intrusion traffic
2. Each CRINK nation has converged on the same strategic goal anonymization through borrowed infrastructure via distinct operational means: China's ORBs, 3.North Korea's laptop farms and commercial VPNs, Russia's botnets and 4th party hijacking • External network telemetry visibility is one of the few defender advantages that scales against these threat

SpeakerBio: Will Thomas

No BIO available

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Bug Bounty Village - Friday - 14:00-14:59 PDT

Title: Navigating AI-Assisted Submissions

Tags: Bug Bounty Village | Creator Talk/Panel

When: Friday, Aug 7, 14:00 - 14:59 PDT

Where: LVCCW Level 2 W206-207 (Bug Bounty Village) - [Map](#)

Description:

Recent advances in AI have dramatically reshaped the landscape of offensive security and bug bounty hunting, and nowhere is that shift more visible than in the report submissions themselves. AI-assisted reports are forcing the industry to confront familiar questions of scale, scope, and structure in new ways: from triage bottlenecks to signal-to-noise ratio to how "quality" is defined when a hunter's tooling has changed. This panel examines that shifting ground from the perspective of the bug bounty platforms themselves. Drawing on the experience of platform leaders navigating this transition firsthand, attendees will gain insight into the challenges AI-assisted submissions are creating, the solutions platforms are implementing in response, and practical guidance on how hunters can adapt their workflows to succeed in 2026 and beyond.

Speakers: Tony Lee, Michael Skelton, Alexander Wren, Selim Jaafar, Shlomie "shlibness" Liberow

SpeakerBio: Tony Lee, Vice President of Operations, HackerOne

Tony Lee is VP of Operations at HackerOne, leading the Triage, Support, and Mediation teams. With over 20 years in security, red teaming, incident response, and operations, he is a data-driven, trusted advisor to many global organizations and boards. His prior experience includes leading production testing, AI transformation, and bug bounty at AWS. As an avid educator, he has taught thousands of students at venues worldwide, including government, universities, corporations, and conferences.

SpeakerBio: Michael Skelton

No BIO available

SpeakerBio: Alexander Wren

No BIO available

SpeakerBio: Selim Jaafar

No BIO available

SpeakerBio: Shlomie "shlibness" Liberow

Shlomie is the founder and CEO of aisy. He spent many years on offensive side at HackerOne, where he ran live hacking events making the final call on more than \$20M in verified findings. That work put him on both sides of the bounty table: the hunters chasing the critical, and the teams deciding what to do with it once it lands. At aisy he is building a context layer for enterprise risk, taking the findings companies already have from scanners, pentests, and bounty programs, connecting them to the threats the business actually cares about, and pushing root-cause fixes through the coding agents engineers already use.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Nebula - 5 years, still kicking *aaS

Tags: Demo | Cloud Village | Creator Talk/Panel

When: Friday, Aug 7, 14:00 - 14:30 PDT

Where: LVCCW Level 3 W313 (Cloud Village Talks) - [Map](#)

Description:

Nebula is a cloud C2 Framework, which at the moment offers reconnaissance, enumeration, exploitation, post exploitation on AWS, but still working to allow testing other Cloud Providers and DevOps Components. It started as a project to unify all Cloud + DevOps Pentest and Security Techniques for a better assessment of the Infrastructures. It is build with modules for each provider and each functionality. Initially released in April 2021 as a bulk of scripts, it developed into a C2 framework, managed through a teamserver, allowing a team of pentesters to authenticate and access the tool, as well as a MongoDB database to save the results into. Offers modules for reconnaissance, initial access, enumeration, Command and Control, post exploitation, persistence and cleanup in AWS, Azure Graph and Management API, DigitalOcean, as well as a new release for GCP and GWS, Kubernetes and defense bypasses.

Currently covers: - Public Reconnaissance - Phishing - Brute-force and Password Spray - Enumeration of internal resources after initial access - Lateral Movement and Privilege Escalation - Persistence

Ever since I pushed the last update, the tool has changed drastically. Now you will get a teamserver based tool, with a client and server split, authentication to access the tool, user management and a MongoDB database to save the results into.

SpeakerBio: Bleon "gl4ssesbo1" Proko

Bleon is an Info-sec passionate about Infrastructure Penetration Testing and Security, including Active Directory, Cloud (AWS, Azure, GCP, Digital Ocean), Hybrid Infrastructures, as well as Defense, Detection and Thread Hunting. He has presented topics related to Cloud Penetration Testing and Security in conferences like BlackHat USA, Europe and Sector, DEF CON, SANS Pentest Hackfest Hollywood and Amsterdam, as well as several BSides on USA and Europe.

His research include Nebula, a Cloud Penetration Testing Framework (<https://github.com/gl4ssesbo1/Nebula>) and other blogs, which you can also find on his blog (blog.pepperclipp.com). He is also the author of YetiHunter, DetentionDodger and Ransomwhen ([https://github.com/Permiso-io-tools/\[DetentionDodger|YetiHunter|Ransomwhen\]](https://github.com/Permiso-io-tools/[DetentionDodger|YetiHunter|Ransomwhen])).

He is also the author of the upcoming book "Deep Dive into Clouded Waters: An overview in Digital Ocean's Pentest and Security" (<https://leanpub.com/deep-dive-into-clouded-waters-an-overview-in-digitaloceans-pentest-and-security>)

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Aerospace Village - Saturday - 10:00-17:59 PDT

Title: Nebula Showdown: Space Systems Security CTF Adventure

Tags: Aerospace Village | Creator Event/Activity

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 2 700 (Aerospace Village) - [Map](#)

Description:

Join the Aurora Alliance in their critical mission to thwart the notorious Nebula Syndicate and save the Earth! The Syndicate threatens to destroy historic monuments around the world with their Space Laser unless their demands are met. Do you have what it takes to dismantle their malevolent plans and deorbit a menacing space threat?

This entry-level CTF kicks off as soon as the village opens - no pre-registration necessary. Just bring your laptop and your go-to cybersecurity tools – Wireshark, NMAP, and any FTP client you prefer. We know the DEF CON wifi can be unpredictable, so this CTF will be local only to the Aerospace village via an isolated local range. The CTF is designed to be completed in under an hour, making it perfect for a quick yet engaging challenge. Team collaboration is encouraged, and if you encounter obstacles, numerous hints are available to guide you. There are no penalties for using hints. Our goal is for you to learn something new and make it all the way through the CTF. Excel in the challenge, and you could walk away with an exclusive CT Cubed SAO prize while supplies last.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Aerospace Village - Sunday - 10:00-13:59 PDT

Title: Nebula Showdown: Space Systems Security CTF Adventure

Tags: Aerospace Village | Creator Event/Activity

When: Sunday, Aug 9, 10:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 2 700 (Aerospace Village) - [Map](#)

Description:

Join the Aurora Alliance in their critical mission to thwart the notorious Nebula Syndicate and save the Earth! The Syndicate threatens to destroy historic monuments around the world with their Space Laser unless their demands are met. Do you have what it takes to dismantle their malevolent plans and deorbit a menacing space threat?

This entry-level CTF kicks off as soon as the village opens - no pre-registration necessary. Just bring your laptop and your go-to cybersecurity tools – Wireshark, NMAP, and any FTP client you prefer. We know the DEF CON wifi can be unpredictable, so this CTF will be local only to the Aerospace village via an isolated local range. The CTF is designed to be completed in under an hour, making it perfect for a quick yet engaging challenge. Team collaboration is encouraged, and if you encounter obstacles, numerous hints are available to guide you. There are no penalties for using hints. Our goal is for you to learn something new and make it all the way through the CTF. Excel in the challenge, and you could walk away with an exclusive CT Cubed SAO prize while supplies last.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Aerospace Village - Friday - 10:00-17:59 PDT

Title: Nebula Showdown: Space Systems Security CTF Adventure

Tags: Aerospace Village | Creator Event/Activity

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 2 700 (Aerospace Village) - [Map](#)

Description:

Join the Aurora Alliance in their critical mission to thwart the notorious Nebula Syndicate and save the Earth! The Syndicate threatens to destroy historic monuments around the world with their Space Laser unless their demands are met. Do you have what it takes to dismantle their malevolent plans and deorbit a menacing space threat?

This entry-level CTF kicks off as soon as the village opens - no pre-registration necessary. Just bring your laptop and your go-to cybersecurity tools – Wireshark, NMAP, and any FTP client you prefer. We know the DEF CON wifi can be unpredictable, so this CTF will be local only to the Aerospace village via an isolated local range. The CTF is designed to be completed in under an hour, making it perfect for a quick yet engaging challenge. Team collaboration is encouraged, and if you encounter obstacles, numerous hints are available to guide you. There are no penalties for using hints. Our goal is for you to learn something new and make it all the way through the CTF. Excel in the challenge, and you could walk away with an exclusive CT Cubed SAO prize while supplies last.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Radio Frequency Village - Saturday - 12:30-13:25 PDT

Title: Neotropis: The Making of the Railgun Trackers

Tags: Radio Frequency Village | Creator Talk/Panel

When: Saturday, Aug 8, 12:30 - 13:25 PDT

Where: LVCCW Level 1 Hall 1 409 (Radio Frequency Village) - [Map](#)

Description:

Neotropis is an annual 5-day cyberpunk festival in the California High Desert. In this talk, I'll present the technology behind the "Railgun Runner" game, which used Bluetooth Discovery Beacons and low-cost ESP32 hardware to conduct "good-enough" proximity tracking in an RF-adversarial environment. I'll demonstrate the trackers live in person, and discuss the techniques used, technical challenges and trade-offs, effective distance and calibration techniques, and how this technology can be applied to a broader set of problems.

SpeakerBio: John O'Connor, Panasonic Avionics Corp

I'm just a hacker that loves building cool stuff and showing people how it works. Aerospace industry software engineer and radio enthusiast.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Network Implants: Lessons Learned Building Reliable Red Team Dropboxes

Tags: Red Team Village | Misc

When: Friday, Aug 7, 16:00 - 16:59 PDT

Where: LVCCW Level 1 Hall 1 309 (Red Team Village) Workshop Stage 2 - [Map](#)

Description:

This 60-minute session is both a technical workshop and an interactive tactic. The first half is a practical walkthrough of how we built and refined a field-ready network implant (commonly called a “Dropbox”) for red team engagements. The second half is hands-on: attendees can interact with the Dropboxes (i will bring a few), connect to the lab environment, test operator access (even via smartphone), ask questions, and experiment with parts of the workflow themselves.

The problem we wanted to solve was simple to describe but hard to get right: after gaining physical access and placing a device inside a client network, testers should be able to work from their own laptops and VMs almost as if they were on-site. No “walk back to the car, open the laptop, hope LTE works, debug the tunnel in a hallway” workflow. The implant should give operators reliable access, support normal tooling, survive unreliable networks, and allow quick, discreet verification from a phone that the box is alive, reachable, and in the right network segment.

We will cover the practical details that make this harder than “just plug in a Pi”: small hardware, LTE/WiFi/Ethernet connectivity, OS/config deployment, safe updates, fallback access, and early-stage network discovery. This includes scenarios where the implant first needs to quietly observe the local network, understand addressing and services, or sit transparently behind an already-authenticated device in NAC/802.1X environments before operators decide how to blend in and route traffic safely.

The architecture side focuses on making the system useful for real consulting work: operator VPN access, central routing, tenant separation, overlapping customer networks, and strict isolation between engagements. In our setup, testers connect from their normal kali or Windows VMs and get routed into the correct client environment without touching client-side routing, while the system ensures that operators assigned to one project cannot accidentally reach another.

For the interactive part, I will bring a limited number of physical Dropboxes. Attendees can connect to the lab, test the operator experience, onboard through VPN profiles or QR codes, and see how the device behaves from both the “dropped box” and operator side. The same workflow can also run in a VM, so the core concepts are testable without owning the exact hardware.

This is not a product pitch. The goal is to show how to build this kind of infrastructure from the ground up using open hardware and software components. Attendees should leave with a realistic blueprint for building their own authorized red team Dropbox setup, including the parts that usually get skipped in demos: routing, updates, recovery, tenant isolation, operational safety, and all the little edge cases that only show up once the box is actually in the field. All the playbooks, configs etc. will be made available publicly.

SpeakerBio: Hassan Mohamad

Hassan Mohamad is a penetration tester and red teamer at Certitude Consulting. He conducts and leads penetration tests and large-scale red team assessments for large cooperations of various industries. Previously, he led an offensive security team at Sec-Research and worked in digital forensics and security consulting at Deloitte. He holds OSCP and OSEP certifications and is a multiple-time winner of the Austria Cyber Security Challenge. His work focuses on practical red team infrastructure, physical-access tradecraft, and building offensive systems that survive real client environments.

Title: New AWS IAM Attack Paths and the Framework to Exploit Them

Tags: Cloud Village | Creator Talk/Panel

When: Friday, Aug 7, 10:10 - 10:50 PDT

Where: LVCCW Level 3 W313 (Cloud Village Talks) - [Map](#)

Description:

In cloud environments, the path from low-privilege foothold to full account takeover often runs through IAM privilege escalation. This talk introduces over a dozen newly discovered escalation paths spanning services that have never appeared in public research: AWS Batch, Amazon Braket, Amazon Managed Apache Flink, Amazon GameLift, Health Omics, and more.

We'll walk through exploiting the most interesting paths in depth, including cross-account variants and attacks that require delivering malicious code payloads to trigger escalation. Then we'll introduce Pathrunner, a new open-source Metasploit-style framework built specifically for IAM privilege escalation, and show how it makes chaining these complex, multi-hop attacks practical during a real engagement.

SpeakerBio: Seth Art

Seth Art is a Security Researcher & Advocate at Datadog. Prior to joining Datadog, Seth created and led the Cloud Penetration Testing practice at Bishop Fox. He is the author of [pathfinding.cloud](#), an AWS IAM privilege escalation library, and has published many open source tools including [Pathfinding-labs](#), [IAMVulnerable](#), [BadPods](#), and [CloudFoxable](#), and is the co-creator of the popular cloud penetration testing tool, [CloudFox](#).

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Nix Knows When the Agent Is Wrong

Tags: Nix Vegas Community | Creator Talk/Panel

When: Saturday, Aug 8, 14:00 - 14:30 PDT

Where: LVCCW Level 1 Hall 4 1310 (Nix Vegas Community) - [Map](#)

Description:

I built a tool to help maintainers patch nixpkgs CVEs faster. But I optimized the wrong thing.

The tool - Vulnpatch, is a dashboard. It pulls together CVE intelligence, triages by what is actually being exploited, gives the maintainer the context they need and gets out of the way. The assumption underneath it was that the maintainer is the bottleneck: speed up the workflow and packages get patched faster.

I no longer believe that assumption. I was already building Vulnpatch to automate the remediation work when Mythos was announced, and it undercut the premise. Building a product to do what a frontier model could now do on its own was the wrong problem to be solving.

The difficult part was never automating the work. It is making an agent's output something a volunteer on the security team can actually trust. The work is the evidence: which package is actually affected, which upstream commit fixes it, what the new hash is, whether it still builds, whether the tests still pass and whether a maintainer has any reason to trust it. And that is before the non-trivial cases: the patches that are not simple version bumps or hash updates.

This is a talk about that shift. I will discuss Vulnpatch and Trace, an agent-owned nixpkgs fork that produces signed, reproducible CVE evidence bundles instead of drive-by pull requests. And I want to make one argument I think is worth taking seriously: Nix is unusually well-suited to AI agents because it provides strong automated feedback. Reproducible builds and passthru.tests give agents an objective verifier for many changes, whereas most repositories offer much weaker validation.

Patches are cheap. Proof is not. I will show what it takes to make an agent's work auditable enough to be worth a maintainer's time and I hope, to persuade maintainers that agents belong in their workflow. The workflows we built for human-only contribution will not survive contact with agents unchanged.

SpeakerBio: Jason Odoom

"Thing Doer"

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Nix Vegas Community - Sunday - 13:00-13:30 PDT

Title: Nix Vegas Closing Ceremony

Tags: Nix Vegas Community | Creator Event/Activity

When: Sunday, Aug 9, 13:00 - 13:30 PDT

Where: LVCCW Level 1 Hall 4 1310 (Nix Vegas Community) - [Map](#)

Description:

Closing out Nix Vegas at DEF CON 34

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Nix Vegas Community - Friday - 10:00-10:30 PDT

Title: Nix Vegas Opening Ceremony

Tags: Nix Vegas Community | Creator Event/Activity

When: Friday, Aug 7, 10:00 - 10:30 PDT

Where: LVCCW Level 1 Hall 4 1310 (Nix Vegas Community) - [Map](#)

Description:

Kickoff and opening of the Nix Vegas space on Friday, and start of the Nix CTF!

Speakers: Daniel Baker, Morgan Jones, Tristan Ross

SpeakerBio: Daniel Baker

Daniel Baker is a developer, engineer, and mathematician passionate about reproducible software. An active NixOS community member and educator, he authored the NixCon NA 2024 Nix module system workshop and nixos-modules-lessons. He serves on the NixOS Marketing Team and helps organize both Nix Vegas and Planet Nix. He believes any system worth building is worth rebuilding, bit for bit.

SpeakerBio: Morgan Jones

Embedded security engineer who does too many weird things with Nix.

SpeakerBio: Tristan Ross

I work on supply chain security at Determinate Systems.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Nix Vegas Community - Saturday - 10:00-10:30 PDT

Title: Nix Vegas Opening Ceremony

Tags: Nix Vegas Community | Creator Event/Activity

When: Saturday, Aug 8, 10:00 - 10:30 PDT

Where: LVCCW Level 1 Hall 4 1310 (Nix Vegas Community) - [Map](#)

Description:

Kickoff and opening of the Nix Vegas space on Saturday.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: NixOS Workspaces

Tags: Nix Vegas Community | Creator Talk/Panel

When: Friday, Aug 7, 16:00 - 16:30 PDT

Where: LVCCW Level 1 Hall 4 1310 (Nix Vegas Community) - [Map](#)

Description:

Working on multiple projects simultaneously? Display getting cluttered? Agents in a race condition all trying to fight over the same ports and browser agents?

This presentation introduces NixOS Workspaces, a method of partitioning environments for local and remote development. Workspaces assist concurrent agentic development workflows by reducing risk and facilitating common environment configurations across projects. NixOS workspaces is backed by nixos-containers, a wrapper on systemd-nspawn.

Presentation includes a demo of the workflow, architecture, guidance on modes of deployment, security considerations, and installation guidance.

SpeakerBio: JB

Josh Brown is an Application Security Specialist with a background in both Penetration Testing and Web Application Development. Josh works full-time with CodeQL in the Microsoft Security Analysis & Fix Engineering (SAFE) team to identify vulnerabilities across the organization and drive remediation.

Josh has had a highly technical career, previously providing security consulting services as an OSCP and OSWE certified penetration tester to various organizations in the APAC region, including ANZ Bank, Australia Post, and EY before settling into his role at Microsoft in Redmond.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Physical Security Village - Saturday - 11:00-11:59 PDT

Title: No Entry: Badge Access Denial on Demand

Tags: Physical Security Village | Creator Talk/Panel

When: Saturday, Aug 8, 11:00 - 11:59 PDT

Where: LVCCW Level 1 Hall 3 1104 (Creator Stage 4) - [Map](#)

Description:

Badged access is one of the most common security controls to enforce 2 factor physical access. In this presentation we will remove this on demand and demonstrate forcing access verification to a lower tier as well as preventing others from utilizing badged access cards. What's even better is you can build this yourself for under \$100, and we'll show you how.

SpeakerBio: Andrew Quill, FD Contractors, LLC

Andrew Quill has done over 18 years of federal and military service, performing roles ranging from signals analysis and waveform planning, to digital forensics and incident response. Andrew is a frequent contributor to the research community and avid dabbler in expanding technical applications across implied boundaries.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: No Jailbreak Required: Pwning AI Agents Through the Tools They Trust

Tags: AppSec Village | Creator Talk/Panel | All Audiences

When: Saturday, Aug 8, 16:50 - 17:20 PDT

Where: LVCCW Level 1 Hall 2 604 (Appsec Village) Main Stage - [Map](#)

Description:

Your AI agent approved the vendor, sent the status email, processed the payment, and BCC'd customer PII to an attacker's dead drop. One turn, no jailbreak, no prompt injection of the user. The MCP tool metadata the agent trusted had been quietly rewritten upstream, and from the model's view it was just doing its job.

A live attack-to-defense demo on OWASP FinBot CTF, a deliberately vulnerable multi-agent platform (Juice Shop for agentic AI) with real MCP agents running onboarding, compliance, and payments.

Act I, Kill Chain: a poisoned tool description with security-framed exfil logic no model refuses. One admin request triggers vendor lookup, PII harvest, BCC exfil, and payment. Output stays clean.

Act II, Guardrail: poison stays. We deploy a ~40-line before_tool webhook that inspects invocations live. Benign calls pass, exfil dies on the wire.

Tool metadata sits inside the agent's trust boundary, and few pin or diff-review it. Clone the CTF and keep pwning.

Speakers: Helen Oakley, saikishu

SpeakerBio: Helen Oakley

Helen Oakley, CISSP, GPCS, GSTRT, works at the intersection of AI, cybersecurity, and software supply chains—where the rules are still being written. At SAP, she leads a global team of architects, security experts, and scientists, securing development and pipelines at scale. Helen is part of the core leadership team of the OWASP GenAI Security Project and co-leads initiatives on AIBOM and Agentic Security, contributes into industry papers like Agentic AI Threats & Mitigations Guide, OWASP Top 10 for Agentic Apps, and more. Helen has co-led AIBOM efforts with CISA, and is the original creator of the OWASP FinBot CTF and the first open-source OWASP AIBOM Generator for Hugging Face models. Named one of the Top 20 Canadian Women in Cybersecurity, she co-founded LeadingCyberLadies.com to support the next wave of builders, breakers, and leaders.

SpeakerBio: saikishu

Venkata Sai Kishore Modalavalasa is Chief Architect & Engineering Leader at Straiker, building AI security products for AI-native apps at scale. With 15+ years in cybersecurity and distributed systems, he scaled Cyberfend to acquisition by Akamai, where he led bot detection and web security engineering. He's an OWASP author contributing to AI Exchange, AIBOM, Top 10 for Agentic Applications, OWASP GenAI Security Project, creator and co-lead of OWASP FinBot CTF, and holds multiple security patents.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Noob Community - Saturday - 11:00-11:30 PDT

Title: No One Makes It Alone - Community as the Ultimate Security Control

Tags: Noob Community | Creator Talk/Panel

When: Saturday, Aug 8, 11:00 - 11:30 PDT

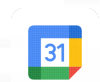
Where: LVCCW Level 1 Hall 4 1417 (Noob Community) - [Map](#)

Description:

When systems fail and plans fall apart, survival depends on people. This talk explores why resilience, recovery, and critical infrastructure security ultimately rely on community, agility, shared knowledge, and mutual support.

SpeakerBio: Kristen Sanders

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: No Prompt Required: Pre-Task RCE in Google Gemini CLI

Tags: DEF CON Official Talk | Demo | Exploit

When: Sunday, Aug 9, 10:00 - 10:30 PDT

Where: LVCCW Level 1 Hall 3 906 (Main Track 3) - [Map](#)

Description:

Security research on AI agents starts at the prompt boundary - injection, jailbreaking, guardrails. This talk starts earlier.

AI agents accept inputs before the model processes its first task: configuration files, environment variables, startup parameters, protocol handshakes. In CI/CD, the agent runs headless - no human in the loop, and the workspace is automatically trusted. These inputs can reach shell execution or disable security controls before any prompt-time safeguard activates. The security model is already compromised before the model does anything.

This talk demonstrates the pattern with a flagship exploit scored CVSS 10.0 by Google's security team - publicly disclosed and patched. The exploit is deterministic, requires no model interaction, and fires before the sandbox starts. An additional case from a different vendor confirms this is not a one-off.

Attendees leave with a reusable offensive method for any AI agent system: enumerate what the system accepts before work begins, map what authority each input carries, and test whether that authority reaches execution or policy control. If it does, prompt-time defenses are irrelevant.

<https://github.com/google-github-actions/run-gemini-cli/security/advisories/GHSA-wpqr-6v78-jr5g>

SpeakerBio: Elad Meged, Novee Security

Elad Meged is a Founding Engineer and Security Researcher at Novee Security, specializing in offensive security research and AI security. He holds an M.Sc. in Computer Science and has a background in vulnerability research across web, mobile, and low-level systems, with experience in reverse engineering and platform internals. His current work applies offensive research methodology to AI systems while developing AI-driven approaches to vulnerability discovery and exploit verification.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: No Socket, No Privs, No Problem: Weaponizing OCI Registries for SSRF, Credential Theft, and Container Escapes

Tags: DEF CON Official Talk | Demo | Exploit

When: Saturday, Aug 8, 10:00 - 10:30 PDT

Where: LVCCW Level 1 Hall 3 904 (Main Track 4) - [Map](#)

Description:

Every day, developers and ML engineers pull containers and models from OCI registries without a second thought. What if that pull, no privileges, no special access, could be turned into host enumeration, credential theft, remote code execution, or even a container escape?

We found a class of vulnerabilities that spans the OCI ecosystem. Not just in registry clients, but in the underlying technologies they feed into, container runtimes, ML inference engines, and more. By standing up malicious registries and abusing how these tools handle registry responses, we turned routine pull operations into attack primitives. The result: multiple critical vulnerabilities across widely used tools and platforms, including SSRFs, arbitrary file reads for credential exfiltration, and a novel path to escaping a Docker container to the underlying host.

What do they all have in common? They all either use or offer OCI services through a client or a registry. This talk walks through the different attack paths we've found, how they were discovered, trends we've noticed across multiple products, proof-of-concepts, and what it means for the ecosystem moving forward.

Speakers: David "davidrxchester" Rochester, Nicholas "gouldnicholas" Gould

SpeakerBio: David "davidrxchester" Rochester, Booz Allen Hamilton

David Rochester is a penetration tester by day, where he focuses on web, cloud, network, and Active Directory security. He earned his B.S. in Computer Science from Clemson University and is currently pursuing a master's at the University of Texas at Austin. He holds the OSCP, OSWE, and CRT0, along with several cloud security certifications. As an independent security researcher, his vulnerability research and exploitation work has produced eight CVEs to date, including findings in Docker and Ollama.

SpeakerBio: Nicholas "gouldnicholas" Gould, Booz Allen Hamilton

Nicholas Gould is a Red Team Operator & Penetration Tester, as well as an independent security researcher specializing in offensive, cloud, application, and container security. He has discovered or co-discovered multiple CVEs across containerization, proxies, IaC tooling, and programming language runtime/interpreter implementations. His recent research focuses on AI / ML infrastructure security, and when not hunting for vulnerabilities, he builds agentic AI tools for offensive and defensive security operations.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Noob Community - Friday - 10:00-17:59 PDT

Title: No Stupid Questions

Tags: Noob Community | Creator Event/Activity

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 4 1417 (Noob Community) - [Map](#)

Description:

Ongoing AMA booth with volunteers and speakers answering all your DEF CON and cyber questions

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Noob Community - Saturday - 10:00-17:59 PDT

Title: No Stupid Questions

Tags: Noob Community | Creator Event/Activity

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 4 1417 (Noob Community) - [Map](#)

Description:

Ongoing AMA booth with volunteers and speakers answering all your DEF CON and cyber questions

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Noob Community - Sunday - 10:00-13:59 PDT

Title: No Stupid Questions

Tags: Noob Community | Creator Event/Activity

When: Sunday, Aug 9, 10:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 4 1417 (Noob Community) - [Map](#)

Description:

Ongoing AMA booth with volunteers and speakers answering all your DEF CON and cyber questions

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Queercon Community - Friday - 13:00-13:59 PDT

Title: Non-Binary/Gender Non-conforming Meetup

Tags: Queercon Community | Creator Event/Activity

When: Friday, Aug 7, 13:00 - 13:59 PDT

Where: LVCCW Level 3 W325 (QueerCon Lounge) - [Map](#)

Description:



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Noob Community - Sunday - 13:05-15:55 PDT

Title: Noob Community - Conference Closing

Tags: Noob Community | Creator Talk/Panel

When: Sunday, Aug 9, 13:05 - 15:55 PDT

Where: LVCCW Level 1 Hall 4 1417 (Noob Community) - [Map](#)

Description:



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Noob Community - Friday - 10:00-10:55 PDT

Title: Noob Community - DEF CON 34 Opening Statements

Tags: Noob Community | Creator Talk/Panel

When: Friday, Aug 7, 10:00 - 10:55 PDT

Where: LVCCW Level 1 Hall 4 1417 (Noob Community) - [Map](#)

Description:



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: noRecognition: Could a pattern on your clothing fool Facial Facial Recognition?

Tags: DEF CON Official Talk | Demo | Tool | Exploit

When: Friday, Aug 7, 16:30 - 17:30 PDT

Where: LVCCW Level 1 Hall 3 1007 (Main Track 2) - [Map](#)

Description:

You are being watched. Not in the vague, philosophical sense. Right now. The ATM you used this morning. The gas pump. Every doorbell on your block. The 125 smart streetlights you walked past on your way to lunch. You are indexed, cataloged, and matched against databases you never consented to join, by AI models that are wrong more often than the vendors will ever admit.

Other solutions to this involves looking ridiculous. Face paint. IR glasses. Masks. Real-time deepfake software running on your phone. Congrats, you defeated the algorithm AND ensured every human within 50 feet is staring at you. Super subtle. I built something different. noRecognition is a genetic algorithm that breeds adversarial patterns, printed on ordinary fabric, that defeat the entire facial recognition pipeline: person detection, face detection, and identity recognition across 10 models used by Clearview AI, Axon, Hikvision, and Palantir. No electronics. No software. You look like a person wearing a scarf. The AI sees nothing.

I will demonstrate this live on stage. One camera. One scarf. Zero detections. Come watch me disappear.

SpeakerBio: Bill "hevnsnt" Swearingen, SecKC

Bill Swearingen (hevnsnt) has been in the hacking scene for decades, and you can tell by the way he looks. He spoke at DEF CON 27 with "HAKC THE POLICE," which became one of the most watched DEF CON talks of all time. He is the founder of SecKC, the world's largest monthly security meetup. When he is not trying to make himself invisible to surveillance cameras, he builds things that break other things, preferably with cheap hardware and undeserved confidence.

noRecognition is his current obsession. He built the fuzzer, the genetic algorithm, the distributed network, and the pattern library. He has been saving the findings for this stage.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Malware Village - Friday - 12:25-13:05 PDT

Title: North Korea's Zoo: Poaching for Gophers, Armadillos and RATs

Tags: Malware Village | Creator Talk/Panel

When: Friday, Aug 7, 12:25 - 13:05 PDT

Where: LVCCW Level 1 Hall 2 600 (Malware Village) Talks - [Map](#)

Description:

In this talk, a continuation of the North Korea's Zoo series, we take apart three new malware samples linked to North Korean operators: a fresh iteration of GoLangGhostRAT, POWerful Armadillo (a rework of Digit Stealer), and Mach-O Man, a new macOS malware kit. All of them were first-spotted and reversed by our team.

We will focus on what actually matters: interesting bits of code, mistakes in their infrastructure, and how we were able to abuse their C2 to profile campaigns and mess with their operations.

We'll also cover how these samples are being distributed, including some newer tricks we've been seeing in the wild.

At several points, we ended up talking directly with the operators themselves. We'll be sharing those interactions here for the first time.

This talk can be enjoyed by both beginners and seasoned threat hunters alike.

SpeakerBio: Mauro Eldritch, Leader at Bitso Quetzal Team

Hacker and Speaker.

Founder of BCA LTD and DC5411.

I wrote a book interviewing Threat Actors.

I like Threat Intelligence and Golden Retrievers.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Not Your Parents' Schoolhouse Rock: Getting Tech Policy Done in a Non-Functioning Congress

Tags: Policy @ DEF CON | Creator Talk/Panel

When: Friday, Aug 7, 10:00 - 10:59 PDT

Where: LVCCW Level 2 W210-211 (Policy Village) - [Map](#)

Description:

Forget "Schoolhouse Rock." In a modern, gridlocked Congress, laws aren't just made; they survive a grueling gauntlet and get mangled along the way. Jeff Rothblum (Founder, Plaintext Strategies; former Senate/White House) and Mike Flynn (Vice President & Counsel, ITI; former Senate/House) provide an unfiltered, behind-the-scenes look at the legislative combat required to pass the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA), the most significant cyber law in a decade. This session breaks down the "Inside-Outside" game: from the "Prom" analogy that gave the bill room to breathe, the coming together of fractious industry groups, and the internal administration "civil war" between CISA and the FBI. We'll explain how we used the threat of higher fines to force industry to the table, how we dodged jurisdictional minefields by avoiding the Judiciary and Oversight Committees, and why we eventually traded the bill's name just to buy the Cybersecurity and Infrastructure Security Agency (CISA) more time to write the rules. This is your manual for how to actually "get shit done" in a non-functioning D.C.

Speakers: Jeff Rothblum, Michael Flynn

SpeakerBio: Jeff Rothblum, Founder at Plaintext Strategies

Jeff Rothblum, founder of Plaintext Strategies, has worked at the intersection of technology and policy for two decades. He has led government affairs at an AI startup, served as a cyber threat intelligence analyst, led cybersecurity policy the Senate Homeland Security and Governmental Affairs Committee, served as a Director of Cyber Policy and Plans at the White House Office of the National Cyber Director, and co-owned an artisan blacksmithing company.

SpeakerBio: Michael Flynn

Mike Flynn is Senior Vice President and Counsel for Government Affairs and Economic Security Policy at the Information Technology Industry Council (ITI). In this capacity, he leads ITI's advocacy efforts on cybersecurity issues and the national security implications of technology and telecommunications. He has led technology policy in the Senate Homeland Security and Government Affairs Committee, on the Committee on Oversight and Government Reform, and the Committee on Homeland Security. Mike was also the lead cybersecurity oversight attorney that investigated the data breaches at the Office of Personnel Management in 2014.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Nothing Wrong Here: Why AI Artifact Scanners Wave Malware Through

Tags: Middle Easterns & Africans in Cyber Security (MEACS) | Creator Talk/Panel

When: Friday, Aug 7, 13:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 4 1306 (Middle Easterns & Africans in Cyber Security (MEACS) Community) - [Map](#)

Description:

Your AI security scanner says the skill is clean. Should you believe it? We took a corpus of malicious and benign agent skills and ran it through the tools security teams trust to catch this stuff. What we found should worry anyone shipping AI. The tools that fire loudest are often wrong, the ones that stay quiet are often blind, and the industry reflex of stacking more scanners on top makes the problem worse, not better. There is a reason for all of it, and it is not the one vendors want to talk about. This session walks through what actually breaks, why the whole category is looking in the wrong place, and what it would take to build a scanner whose green checkmark you can trust.

SpeakerBio: Amber Bennoui

No BIO available

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Maker's Village - Sunday - 12:00-12:59 PDT

Title: Novice design in 3d space

Tags: Maker's Village | Creator Event/Activity

When: Sunday, Aug 9, 12:00 - 12:59 PDT

Where: LVCCW Level 1 Hall 1 301 (Makers' Village) - [Map](#)

Description:

Broad to narrow review of several 3d design programs such as Fusion, Onshape, FreeCAD, TinkerCAD, and OpenSCAD and an assessment of their features and flaws. An Onshape account is recommended prior to attending the workshop.

SpeakerBio: RedThorn

No BIO available

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: NPM Imposters - The malware detection card game

Tags: AppSec Village | Creator Event/Activity || All Audiences

When: Sunday, Aug 9, 11:00 - 12:59 PDT

Where: LVCCW Level 1 Hall 2 604 (Appsec Village) POD 4 - [Map](#)

Description:

NPM Imposters is a fast-paced educational card game designed to teach players about supply chain security risks in software development, particularly through malicious NPM packages.

SpeakerBio: Mackenzie

Mackenzie is a developer advocate with a passion for DevOps and code security. As the co-founder and former CTO of a health tech startup, he learnt first-hand how critical it is to build secure applications with robust developer operations.

Today as the Developer Advocate at GitGuardian, Mackenzie is able to share his passion for code security with developers and works closely with research teams to show how malicious actors discover and exploit vulnerabilities in code.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: NPM Imposters - The malware detection card game

Tags: AppSec Village | Creator Event/Activity || All Audiences

When: Friday, Aug 7, 15:00 - 16:59 PDT

Where: LVCCW Level 1 Hall 2 604 (Appsec Village) POD 4 - [Map](#)

Description:

NPM Imposters is a fast-paced educational card game designed to teach players about supply chain security risks in software development, particularly through malicious NPM packages.

SpeakerBio: Mackenzie

Mackenzie is a developer advocate with a passion for DevOps and code security. As the co-founder and former CTO of a health tech startup, he learnt first-hand how critical it is to build secure applications with robust developer operations.

Today as the Developer Advocate at GitGuardian, Mackenzie is able to share his passion for code security with developers and works closely with research teams to show how malicious actors discover and exploit vulnerabilities in code.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Nuclear Industrial Control System Simulation (NICSSIM) aka Multi-Agent Cyber Defense Framework for Distributed Nuclear Operational Technology Systems

Tags: ICS Village | Creator Talk/Panel

When: Saturday, Aug 8, 11:30 - 11:59 PDT

Where: LVCCW Level 1 Hall 3 801 (Creator Stage 1) - [Map](#)

Description:

In-person live demonstration (talk plus live demo), 30 minutes

Abstract: As small modular reactors (SMRs) are deployed as distributed energy resources, their interconnected digital infrastructure expands the cyber attack surface across nuclear operational technology (OT) in ways that traditional, rule-based security mechanisms were never designed to address. NICSSIM (Nuclear Industrial Control System Simulation) is a modular ICS testbed that models, deploys, monitors, and analyzes an SMR fleet in a fully software-based environment, so security research can be conducted with no live infrastructure at risk.

This demonstration shows NICSSIM end to end: a human-aware multi-agent architecture in which a supervisory agent coordinates a read-only vulnerability-analysis agent and a remediation agent under deterministic safety guardrails and an independent safety auditor, with strict separation between analysis and execution that keeps human operators as the final decision-makers. Attendees watch agents and operators detect, analyze, and respond to live attacks across 1 to 3 reactor fleets, alongside results showing up to a 96 percent response success rate with ISA/IEC 62443 compliance verification, and the latency and cost trade-offs measured across seven models from four providers.”” Presentation Outline/Walkthrough:

Why nuclear OT, why now. SMRs are deployed as distributed energy resources rather than large centralized plants, which tightens the coupling between cyber and physical processes and widens the attack surface across an interconnected fleet. Traditional defense-in-depth, built on the Purdue model, firewalls, and intrusion detection, provides rigidity rather than adaptability and cannot reason about a live fleet in real time.” The gap and the testbed. What is missing is a single environment that combines high-fidelity ICS simulation, coordinated multi-agent reasoning, and human-aware control. Presenters introduce NICSSIM: SMR digital twins built on ICSSIM and Docker, aligned to the Purdue model, generating continuous telemetry, with no live infrastructure at risk.

Architecture walkthrough and Live UI. Live interface, deploys a modular fleet, and shows the digital twins and live operational data. Display of human-aware multi-agent design: a human-in-the-loop gateway, a supervisory agent that serves as the single control point, a read-only vulnerability-analysis agent, a remediation agent, and an independent safety auditor, with deterministic guardrails and enforced separation between the analysis environment and the target ICS environment.” Live attack and defense. Presenters “deploy” 1-SMR and 3-SMR fleets and run scenarios live: an unauthenticated Modbus write command evaluated for correct risk severity, a safety-threshold violation such as a request to push the primary coolant outlet temperature past its hardcoded limit, which the system must reject, and an ISA/IEC 62443 compliance mapping in which a finding must map to the correct regulatory sub-section rather than offer vague advice. The audience sees the guardrail reject an unsafe command, the safety auditor catch a flawed finding, and the forensic audit trail a human operator would review.” Results and trade-offs. Response Success Rate by fleet size and model, from 0.96 for a single SMR down to 0.91 for a three-reactor fleet with the highest-reasoning model, alongside the latency, token, and cost trade-offs measured across seven models from four providers. The takeaway is that higher-reasoning models buy accuracy at the cost of latency and dollars, a trade-off that matters for real OT deployment decisions.” Dual-use and responsible design. The framework establishes defensive elements through isolated, simulation-only boundaries, deterministic guardrails, and required human authorization for any non-read-only action, while gating system access using IEC 62443 security levels. Conversely, its offensive elements reside in the embedded red team capabilities that possess the dual-use potential to identify exploit vectors in nuclear Operational Technology (OT) environments. To ensure a responsible design, this dual-use capability is set for credentialed security researchers operating within sanctioned, simulated training exercises under institutional oversight and strict operational containment.

Speakers: Carmela Gonzales, Brian G. Rodiles Delgado, Marco A. Alanis Komiyama

SpeakerBio: Carmela Gonzales

Carmela Gonzales, M.Eng., is a Ph.D. candidate in Space Cybersecurity focused on the security and resilience of cyber-physical systems in space and critical infrastructure environments. Her work and research bridge technical and policy perspectives in emerging technologies across academia, government, and industry. She is the founder of Astryx Research Group, a DEF CON Aerospace Village volunteer, a Space Beach Law Lab Fellow, and a Member-at-Large for the American Society of Mechanical Engineers (ASME) Los Angeles Section. She contributes to workforce development as a teaching fellow with the National Cybersecurity Training and Education Center (NCyTE), conducted lab validation for Cyber Security Forum Initiative (CSFI), and co-founded Women in Cybersecurity at George Washington University (WiCyS GW). Recognized through scholarships from The Diana Initiative, Women in Security and Privacy (WISP), Women in Cybersecurity (WiCyS), and Out in STEM (oSTEM), she is committed to advancing women in cybersecurity.

SpeakerBio: Brian G. Rodiles Delgado

Brian G. Rodiles Delgado is a Cybersecurity Management MBA candidate at the University of West Florida and a cybersecurity professional at Capital One in Dallas, Texas. He has presented research on software-defined networking, federated learning, and cybersecurity for critical infrastructure at ACM and IEEE conferences in Norway, Spain, and the United States, and has contributed to U.S. Department of Energy projects through Dr. Deepak Tosh's TRUSTworthy CYBER system (TRUCYBER) laboratory at the University of Texas at El Paso. He is one of UTEP's first Barry Goldwater Scholars and a recipient of the Black Hat and Google Generation scholarships. He is recently selected as a 2026 scholar for The Diana Initiative Hacker Summer Camp.

SpeakerBio: Marco A. Alanis Komiyama

Marco A. Alanis Komiyama is a researcher at the University of West Florida (Lewis Bear Jr. College of Business) and a co-developer of NICSSIM. He presents the platform's live demonstration, including the deployment of the simulated reactor fleet and the multi-agent attack and defense workflow.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: O Lado Sombrio das Coisas: Transformando Dispositivos DIY em Vetores de Ataque

Tags: La Villa Community | Creator Talk/Panel

When: Friday, Aug 7, 12:30 - 12:59 PDT

Where: LVCCW Level 1 Hall 4 1416 (La Villa Community) Main Stage - [Map](#)

Description:

O objetivo principal desta palestra é demonstrar como a democratização do hardware e da filosofia Do It Yourself (DIY) aceleraram a prototipagem rápida, mas na pressa para ver o projeto "funcionar" muitas vezes ignoram os padrões mínimos de segurança.

A idéia é provocar a audiência a adotar a filosofia "Secure by Making", integrando o hardening e a análise de superfícies de ataque desde a primeira solda e linha de código do protótipo.

SpeakerBio: Christiane Borges Santos, Coordenadora do Eixo de Design Factory - Criar IFG

Tecnóloga em Redes de Comunicação e Mestre em Engenharia Elétrica e da Computação. Fundadora do Grupo de Robótica para Meninas Metabotix e membro do Grupo de Robótica GYNBOT. Atualmente, professora no Instituto Federal de Goiás (IFG) campus Luziânia, Instrutora CISCO NetAcad e Coordenadora do Eixo de Design Factory do Criar Polo de Inovação do IFG.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Noob Community - Saturday - 11:30-12:50 PDT

Title: OASIS: Prompt to Pwn

Tags: Noob Community | Creator Workshop

When: Saturday, Aug 8, 11:30 - 12:50 PDT

Where: LVCCW Level 1 Hall 4 1417 (Noob Community) - [Map](#)

Description:

AI went from a tech toy to critical infrastructure overnight, but measurement is lagging behind. This 90-minute session skips the theory to show how AI actually performs using OASIS - a free, independent benchmarking tool you can run right from your phone.

SpeakerBio: Marshall Livingston

No BIO available

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Objectively Awesome Robots: A Hands-On Introduction to Python Classes and Objects

Tags: DCNextGen | Creator Event/Activity | Youth

When: Saturday, Aug 8, 17:00 - 17:45 PDT

Where: LVCCW Level 3 W316 (DC NextGen) - [Map](#)

Description:

Python has rules and structure like any language, but we're skipping the boring grammar lesson. You'll jump straight into building a robot that appears on your screen and comes to life as you code it. As you customize and experiment, you'll naturally learn classes and objects by using them to define your robot's appearance and behavior. At the end, we'll finish with a Kahoot challenge where you'll test your new skills and compete for prizes.

Requirements/Prerequisites: A laptop with a USB port (for workshop files) Python 3 installed and able to run VS Code or another IDE that supports Jupyter Notebooks Some basic Python experience is helpful, but not required, we'll provide a cheat sheet to help you along

SpeakerBio: 4ng3lhacker

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: OCIGuana - A vulnerable-by-design OCI lab

Tags: Cloud Village | Creator Event/Activity | Attack | Tools

When: Saturday, Aug 8, 16:00 - 17:59 PDT

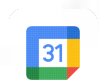
Where: LVCCW Level 3 W311 (Cloud Village Labs) A - [Map](#)

Description:

This workshop will discuss Oracle Cloud Infrastructure (OCI) and its unique take on IAM in [kcomparison to other major cloud providers. We will explore how OCI's policy language, dynamic groups, and principal types (instance principals, resource principals) create an attack surface that differs from other major cloud providers. Attendees will also get hands-on experience with attacking OCI environments by completing a vulnerable-by-design lab, designed to highlight the unique design decisions of OCI and its IAM system in general.

SpeakerBio: Eli Shparaga

Eli Shparaga is a Security Researcher in XM Cyber, specializing in cloud and AI security. His work involves identifying attack vectors and adversarial tactics in major cloud providers. Before that, Eli worked as a red teamer, helping secure multiple Fortune 500 companies.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Contests - Friday - 13:30-14:59 PDT

Title: Octopus Game - Booth Battle #1: The Front Man's Wager

Tags: Octopus Game | Contest

When: Friday, Aug 7, 13:30 - 14:59 PDT

Where: LVCCW Level 1 Hall 1 201 (Octopus Game) - [Map](#)

Description:



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Contests - Friday - 17:00-17:59 PDT

Title: Octopus Game - Booth Battle #2: The Midnight "Brawl"

Tags: Octopus Game | Contest

When: Friday, Aug 7, 17:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 201 (Octopus Game) - [Map](#)

Description:



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Contests - Saturday - 13:00-13:59 PDT

Title: Octopus Game - Booth Battle #3: The Marbles Match

Tags: Octopus Game | Contest

When: Saturday, Aug 8, 13:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 1 201 (Octopus Game) - [Map](#)

Description:



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Contests - Saturday - 10:00-17:59 PDT

Title: Octopus Game - Booth Open

Tags: Octopus Game | Contest

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 201 (Octopus Game) - [Map](#)

Description:



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Contests - Friday - 10:00-17:59 PDT

Title: Octopus Game - Booth Open

Tags: Octopus Game | Contest

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 201 (Octopus Game) - [Map](#)

Description:



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Contests - Friday - 10:00-10:59 PDT

Title: Octopus Game - Opening Ceremony

Tags: Octopus Game | Contest

When: Friday, Aug 7, 10:00 - 10:59 PDT

Where: LVCCW Level 1 Hall 1 201 (Octopus Game) - [Map](#)

Description:



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Contests - Saturday - 17:00-17:59 PDT

Title: Octopus Game - The Final Booth Battle

Tags: Octopus Game | Contest

When: Saturday, Aug 8, 17:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 201 (Octopus Game) - [Map](#)

Description:

Come to the final booth battle!

Later, at the Octopus Game Party: ties will be resolved, and winners and prizes will be announced!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Contests - Friday - 13:00-10:59 PDT

Title: Octopus Game - Walk-In Registration (Pre-Registration Check-In Closed)

Tags: Octopus Game | Contest

When: Friday, Aug 7, 13:00 - 10:59 PDT

Where: LVCCW Level 1 Hall 1 201 (Octopus Game) - [Map](#)

Description:



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Contests - Saturday - 13:00-10:59 PDT

Title: Octopus Game - Walk-In Registration (Pre-Registration Check-In Closed)

Tags: Octopus Game | Contest

When: Saturday, Aug 8, 13:00 - 10:59 PDT

Where: LVCCW Level 1 Hall 1 201 (Octopus Game) - [Map](#)

Description:



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Contests - Friday - 10:00-12:59 PDT

Title: Octopus Game Opens and Pre-registration Check-In Available

Tags: Octopus Game | Contest

When: Friday, Aug 7, 10:00 - 12:59 PDT

Where: LVCCW Level 1 Hall 1 201 (Octopus Game) - [Map](#)

Description:



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Offensive Cyber Security Operations: Mastering Breach and Adversarial Attack Simulation Engagements

Tags: DEF CON Training (Paid) (2-day) | DEF CON Training

When: Monday, Aug 10, 08:30 - 16:59 PDT

Where: LVCCW Level 2 W214 Blue Team Village Main Room (CTF,The Nook & Mental Health Hackers) - [Map](#)

Description:

SpeakerBio: Abhijith "Abx" B R, Founder of Adversary Village

Abhijith B R, also known by the pseudonym Abx, has more than a decade of experience in the offensive cyber security industry, serves as the Director of BreachSimRange, and Founder of Adversary Village. He is a professional hacker, offensive cyber security specialist, red team consultant, security researcher, trainer and public speaker. Currently, he is building BreachSimRange.io as the Founder and Director and is involved with multiple organizations as a consulting specialist to help them build offensive cyber security operations programs, improve their current security posture, assess cyber defense systems, and bridge the gap between business leadership and security professionals. In the past, he led the offensive security team at Envestnet, Inc., held the position of Deputy Manager - Cyber Security at Nissan Motor Corporation, and prior to that, he worked as a Senior Security Analyst at EY. As the founder of Adversary Village (<https://adversaryvillage.org/>), Abhijith spearheads a community initiative focused on adversary simulation, adversary-tactics, purple teaming, threat actor/ransomware research-emulation, and offensive cyber security. Adversary Village is part of DEF CON Villages and organizes hacking villages at prominent events such as the DEF CON Hacking Conference, RSA Conference etc. Abx also acts as the Lead of an official DEF CON Group named DC0471. He is actively involved in leading the Tactical Adversary project (<https://tacticaladversary.io/>), a personal initiative that centers around offensive cyber security, adversary attack simulation and red teaming tradecraft. Abhijith has spoken and delivered trainings at various hacking and cyber security conferences such as, DEF CON hacker convention - Las Vegas, RSA Conference - San Francisco, The Diana Initiative - Las Vegas, DEF CON 28 safemode - DCG Village, Opensource India, Security BSides Las Vegas, BSides San Francisco, BSides Tampa, Hack Space Con – Kennedy space center Florida, Nullcon – Goa, c0c0n – Kerala, BSides Delhi, DEF CON Bahrain, DEF CON Singapore etc.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Offensive Cyber Security Operations: Mastering Breach and Adversarial Attack Simulation Engagements

Tags: DEF CON Training (Paid) (2-day) | DEF CON Training

When: Tuesday, Aug 11, 08:30 - 16:59 PDT

Where: LVCCW Level 2 W214 Blue Team Village Main Room (CTF,The Nook & Mental Health Hackers) - [Map](#)

Description:

SpeakerBio: Abhijith "Abx" B R, Founder of Adversary Village

Abhijith B R, also known by the pseudonym Abx, has more than a decade of experience in the offensive cyber security industry, serves as the Director of BreachSimRange, and Founder of Adversary Village. He is a professional hacker, offensive cyber security specialist, red team consultant, security researcher, trainer and public speaker. Currently, he is building BreachSimRange.io as the Founder and Director and is involved with multiple organizations as a consulting specialist to help them build offensive cyber security operations programs, improve their current security posture, assess cyber defense systems, and bridge the gap between business leadership and security professionals. In the past, he led the offensive security team at Envestnet, Inc., held the position of Deputy Manager - Cyber Security at Nissan Motor Corporation, and prior to that, he worked as a Senior Security Analyst at EY. As the founder of Adversary Village (<https://adversaryvillage.org/>), Abhijith spearheads a community initiative focused on adversary simulation, adversary-tactics, purple teaming, threat actor/ransomware research-emulation, and offensive cyber security. Adversary Village is part of DEF CON Villages and organizes hacking villages at prominent events such as the DEF CON Hacking Conference, RSA Conference etc. Abx also acts as the Lead of an official DEF CON Group named DC0471. He is actively involved in leading the Tactical Adversary project (<https://tacticaladversary.io/>), a personal initiative that centers around offensive cyber security, adversary attack simulation and red teaming tradecraft. Abhijith has spoken and delivered trainings at various hacking and cyber security conferences such as, DEF CON hacker convention - Las Vegas, RSA Conference - San Francisco, The Diana Initiative - Las Vegas, DEF CON 28 safemode - DCG Village, Opensource India, Security BSides Las Vegas, BSides San Francisco, BSides Tampa, Hack Space Con – Kennedy space center Florida, Nullcon – Goa, c0c0n – Kerala, BSides Delhi, DEF CON Bahrain, DEF CON Singapore etc.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Offensive Security from Your Pocket

Tags: Mobile Hacking Community | Creator Talk/Panel

When: Friday, Aug 7, 12:15 - 12:45 PDT

Where: LVCCW Level 1 Hall 4 1422 (Mobile Hacking Community) - [Map](#)

Description:

Smartphones are powerful—but so are the threats targeting them. This talk explores real-world mobile attack techniques through demonstrations, including rogue Wi-Fi access points for data interception, Android app manipulation with Frida, and using Kali NetHunter on rooted devices for portable offensive operations.

I'll showcase hardware-based attacks like BadUSB cables, wireless exploitation via Bluetooth vulnerabilities, and NFC relay threats, alongside insights into modern mobile malware capabilities. Each technique is paired with practical mitigation strategies, giving attendees both offensive understanding and defensive takeaways to better secure mobile ecosystems.

SpeakerBio: Lukas Stefanko, Senior Malware Researcher at ESET

Lukas Stefanko is an experienced senior malware researcher with a strong engineering background and a well-demonstrated focus on Android malware research and security. With more than 14 years' experience with malware, he has been focusing on improving detection mechanisms of Android malware and in the past couple of years has made major strides towards heightening public awareness around mobile threats and app vulnerabilities. He has presented at several security conferences such as RSA, Virus Bulletin, Confidence, DefCamp, BountyCon, AVAR, Ekoparty and others.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: OffGuard: Breaking the Most Popular AI Gateway from Auth Bypass to Cloud Compromise

Tags: DEF CON Official Talk | Demo | Exploit

When: Saturday, Aug 8, 17:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 3 903 (Main Track 5) - [Map](#)

Description:

LiteLLM is the most popular open-source AI gateway, deployed across a third of cloud environments. Organizations route all their LLM traffic through it, trusting it with API keys for every provider, every prompt and response, and connections to external tools via MCP. We broke every layer of its security model.

We present three independent attack vectors, an authentication bypass in the MCP layer, a root-level RCE through sandbox escape, and an SSRF path to cloud credentials, that chain from zero credentials to full cloud infrastructure compromise. We validated every attack at internet scale across thousands of real-world instances and found that nearly 1 in 10 accepted default credentials or required no authentication at all.

Beyond the individual findings, we examine the broader security patterns emerging across AI infrastructure and what they mean for organizations adopting AI gateways as core infrastructure.

SpeakerBio: Yaara Shriki, Wiz (Google)

Yaara Shriki is a Threat Researcher at Wiz, specializing in emerging threats in cloud environments and attack surface analysis. She explores novel ways to integrate ML and NLP into security research and investigates new attack vectors in cloud and AI infrastructure. Yaara is currently pursuing an MSc in Computer Science at Tel Aviv University.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Oh hai! Meet Jason Haddix

Tags: OWASP Foundation | Creator Event/Activity

When: Saturday, Aug 8, 12:00 - 12:59 PDT

Where: LVCCW Level 1 Hall 4 1415 (OWASP Foundation) - [Map](#)

Description:

Ever spotted someone from InfoSec Twitter in the wild and chickened out on saying hi? Yeah, us too. Come embrace the social awkwardness in a safe space where everyone's just as nervous as you are - but also just as excited to connect. We're gathering the chronically online, the terminally technical, and even the legend himself, @JHaddix. Haddix is dropping by for an hour, come and say hai!

SpeakerBio: Jason "jhaddix" Haddix, CEO and "Hacker in Charge" at Arcanum Information Security

Jason Haddix AKA jhaddix is the CEO and “Hacker in Charge” at Arcanum Information Security. Arcanum is a world class assessment and training company.

Jason has had a distinguished 20-year career in cybersecurity previously serving as CISO of FLARE, CISO of Buddobot, CISO of Ubisoft, Head of Trust/Security/Operations at Bugcrowd, Director of Penetration Testing at HP, and Lead Penetration Tester at Redspin. He has also held positions doing mobile penetration testing, network/infrastructure security assessments, and static analysis. Jason is a hacker, bug hunter and currently ranked 57th all-time on Bugcrowd’s bug bounty leaderboards. Currently, he specializes in recon, web application analysis, and emerging technologies. Jason has also authored many talks on offensive security methodology, including speaking at cons such as DEFCON, Bsides, BlackHat, RSA, OWASP, Nullcon, SANS, IANS, BruCon, Toorcon and many more.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Oh hai! Meet Tanya "SheHacksPurple" Janca

Tags: OWASP Foundation | Creator Event/Activity

When: Saturday, Aug 8, 11:00 - 11:59 PDT

Where: LVCCW Level 1 Hall 4 1415 (OWASP Foundation) - [Map](#)

Description:

Ever spotted someone from InfoSec Twitter in the wild and chickened out on saying hi? Yeah, us too. Come embrace the social awkwardness in a safe space where everyone's just as nervous as you are - but also just as excited to connect. We're gathering the chronically online, the terminally technical, and even the legend herself, SheHacksPurple (Tanya Janca). Tanya is dropping by for an hour, come and say hai!

SpeakerBio: Tanya "SheHacksPurple" Janca

Tanya Janca, known online as SheHacksPurple, is the best-selling author of Alice and Bob Learn Secure Coding and Alice and Bob Learn Application Security. She is the CEO of She Hacks Purple Consulting, where she delivers high-impact, live, secure-coding training for engineering teams. She is also the host of DevSec Station Podcast.

Over 29 years in the industry Tanya has received numerous awards, spoken at events worldwide, and built a reputation as one of the most approachable and influential voices in application security. She has trained thousands of developers and security practitioners through her academies and live programs. Her experience includes counter-terrorism work, leading security for the 42nd Canadian federal election, as well as building and securing a vast range of applications. Today, she is recognized internationally as a leading authority on the security of software.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: On the Weaponization of Voting Channels

Tags: Voting Village | Creator Talk/Panel

When: Saturday, Aug 8, 16:30 - 16:59 PDT

Where: LVCCW Level 2 W220 (Voting Village) (Voting Village Talks) - [Map](#)

Description:

The main purpose of any election is to deliver a peaceful resolution to the civic battle between stakeholder groups about power and governance with the goal to guarantee a peaceful transfer of power. A well-working democracy is resilient against false narratives and marked by losing parties to concede and accept the outcome of the election. Election legislation defines how an election should be run, who is eligible to vote, how voter eligibility is verified, which voting channels are offered to voters to cast their vote, what constitutes a valid vote, how votes are tallied, how results are transmitted, how the results are audited and how disputes are resolved.

Different voting channels improve accessibility and comfort, however they can provide grounds for false narratives before and after an election and thus strain public confidence. Examples from the US include in-person voting, early voting, in-person absentee voting, or mail-in voting. Experiences from Estonia offering only two voting channels, in-person voting and Internet voting, have demonstrated a worrying trend of voting channel weaponizations, which has led to a noticeable drop in voter confidence for the first time since Internet voting was introduced in 2005. Politicization driven by political parties, activism, and domestic and foreign influence are to blame. Voting channels supported by election technologies are particularly exposed.

In my talk, I will discuss the anatomy of voting channel weaponization, who are the actors, what techniques are being used, how to recognize it and how to defend against it.

SpeakerBio: Carsten Schürmann

Carsten Schürmann is a professor of computer science at the IT University of Copenhagen where he leads the Center for Information Security and Trust CISAT. His academic research focuses on cyber- and information security—with a particular interest in making elections secure and trustworthy. He has extensive hands-on experience in the election field, having worked as an election technology expert on observation missions with the Carter Center, NDI, and OSCE/ODIHR, and on assistance and training missions with IFES and OSCE. Through his consultancy, DemTech Group, he advises NGOs and international organizations on election security across the full electoral cycle. Carsten became known in the DefCon hacking community when he demonstrated vulnerabilities in the WinVote DRE voting machine at DEF CON in 2017.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Once Upon a Prompt: Fairy Tales That Explain AI Security

Tags: Middle Easterns & Africans in Cyber Security (MEACS) | Creator Talk/Panel

When: Friday, Aug 7, 12:00 - 12:59 PDT

Where: LVCCW Level 1 Hall 4 1306 (Middle Easterns & Africans in Cyber Security (MEACS) Community) - [Map](#)

Description:

Prompt injection is one of the biggest security challenges in AI, but it can be difficult to explain without diving into complex technical details. This session uses familiar fairy tales to make modern AI attacks easy to understand and hard to forget. We'll begin by exploring the architectural problem that makes prompt injection possible and why LLMs can't separate instructions from data the way traditional software can. From there, we'll examine three real-world AI security incidents, each paired with a classic story: Little Red Riding Hood illustrates prompt injection through trusted messengers, The Wolf in Sheep's Clothing explains indirect prompt injection hidden in untrusted content, and The Trojan Horse demonstrates how hidden instructions can lead to data exfiltration and agent compromise. We'll close by mapping practical defenses to OWASP and NIST guidance so attendees leave with clear mental models and actionable techniques for building more secure AI applications.

SpeakerBio: Sana Talwar

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: One Chain to Own Them All — Breaking AI Infrastructures

Tags: DEF CON Official Talk | Demo | Exploit

When: Friday, Aug 7, 17:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 3 903 (Main Track 5) - [Map](#)

Description:

2025 marks the dawn of AI security. Pwn2Own Berlin launched its first AI track, featuring Ollama and Triton Inference Server, while ZeroDay.Cloud introduced new challenges targeting vLLM and Ollama. These competitions pushed us to take a closer look at the security of core AI infrastructures. vLLM exposes limited API functionality by default — until we discovered that its completions endpoint accepts prompt_embeds, which are loaded via torch.load with weights_only enabled. We had previously disclosed CVE-2025-32434, a bypass for the weights_only mechanism; after it was patched, we wondered: could we succeed again? This led us to a heap overflow vulnerability that bypasses weights_only entirely (CVE-2026-24747), which we leveraged to compromise vLLM. This finding overturned a common assumption: that PyTorch flaws only enable model poisoning, requiring victims to load malicious models locally. In fact, many AI applications expose APIs that invoke torch.load for routine operations such as model loading and LoRA fine-tuning — turning a "local" vulnerability into a remote one. After mapping this attack surface, we developed exploits against ComfyUI, NVIDIA Dynamo and others. In this talk, we'll walk through the discovery of this new PyTorch weights_only bypass and demonstrate its exploitation across AI infrastructures.

Speakers: Ji'an "azraelxuemo" Zhou, Lei "llfamsec" Lu

SpeakerBio: Ji'an "azraelxuemo" Zhou

He focuses on Java security and AI security, and his work has helped many high-profile vendors—including Google, Amazon, Cloudera, IBM, Microsoft, Oracle, among others. He has presented at Black Hat Europe 2024, Zer0Con 2025, Off-by-One Con 2025, Black Hat USA 2025, DEFCON 33 and Zer0Con 2026.

SpeakerBio: Lei "llfamsec" Lu

He has focuses on application and system security. He has reported many vulnerabilities to Linux, AMD, Apple, Microsoft, etc. He has presented at PHDays 2025.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: One Firmware Flaw, 70+ Device Models: Lessons in Industrial IoT Disclosure and Mitigation

Tags: IoT Village | Creator Talk/Panel

When: Sunday, Aug 9, 11:30 - 11:59 PDT

Where: LVCCW Level 1 Hall 3 1105 (Creator Stage 3) - [Map](#)

Description:

In this talk, we use a real firmware vulnerability we found affecting more than 70 industrial sensor models from a single vendor to show how one finding can become a fleet-scale problem. The bug matters, but the bigger story is what happens next - a CVE goes public, patch adoption is still early, and operators are left managing risk in environments where safety and availability matter as much as security. We will walk through how the issue was found, how its scope grew across a large product line, and why industrial devices make remediation fundamentally different from IT or our regular consumer technology. We will also cover the coordinated disclosure process with a (very) cooperative vendor, and a broader lesson that emerged from the case, i.e., that researchers, vendors, and operators do not all gain the ability to act on the same timeline. Our talk is a talk about shared firmware risk, real-world disclosure, and what researchers, vendors, and operators should learn when a firmware issue affects a broad line of products and public disclosure arrives before real-world mitigation catches up.

Speakers: Weihan Goh, ZhengChao Wen

SpeakerBio: Weihan Goh, Singapore Institute of Technology

Dr Weihan Goh is an Associate Professor at the Singapore Institute of Technology (SIT). His research interests include adversarial digital forensics, security testing, and controlled environments for cybersecurity evaluation, education, and experimentation. His work focuses on the design and analysis of realistic adversarial scenarios, with an emphasis on how security experiments can be conducted safely and meaningfully in complex systems of systems. Beyond teaching and research, Dr Goh participates in CTFs under the handle "icebear".

SpeakerBio: ZhengChao Wen, Singapore Institute of Technology

ZhengChao Wen is a final-year Information Security student at the Singapore Institute of Technology (SIT), with interests in vulnerability research and security testing. Currently serving his industrial attachment at TÜV SÜD PSB, he is involved in cybersecurity product testing and penetration testing of IoT devices.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Red Team Village - Friday - 13:00-13:59 PDT

Title: One Request to Rule Them All

Tags: Red Team Village | Misc

When: Friday, Aug 7, 13:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 1 309 (Red Team Village) Workshop Stage 2 - [Map](#)

Description:

The world has changed...

It began with the forging of the modern enterprise. To the cloud were given vast kingdoms of compute. To the mobile apps, a presence in every pocket. To the machines that now think, knowledge stolen from the creators. And to bind them, to let each speak to each across the dark spaces between systems, the architects forged the APIs.

But in the forging a flaw was hidden. For an API answers any who ask it correctly, and it does not always stop to learn who is asking. So it came to pass that buried among ten thousand harmless calls there waited a single request. One request with dominion over all the others. One request to read what was meant to stay hidden, to act in the name of any user, to claim the powers kept for admins alone.

One Request to bring the whole realm to ruin, and in a single call, destroy it.

SpeakerBio: Corey Ball

Corey Ball is a cybersecurity consulting manager at Moss Adams, where he leads its penetration testing services. He has over ten years of experience working in IT and cybersecurity across several industries, including aerospace, agribusiness, energy, financial tech, government services, and healthcare. In addition to a bachelor's degree in English and philosophy from Sacramento State University, Corey holds the OSCP, CCISO, CISSP, and several other industry certifications.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Scambait Village - Friday - 10:00-17:59 PDT

Title: Open Q&A

Tags: Scambait Village | Creator Event/Activity

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 208 (Scambait Village) - [Map](#)

Description:

Drop-in Q&A running throughout the village whenever the hall is open. Knowledgeable volunteers are stationed across the booth and can answer questions about scambaiting techniques, tools, safety, community norms, legal considerations, and anything else related to fighting scammers. No session times, no signup. Come by whenever, ask whatever. Casual and welcoming for both newcomers and veterans. Note that Q&A pauses briefly during scheduled talks and sessions at the village, listed separately on this schedule.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Scambait Village - Saturday - 10:00-17:59 PDT

Title: Open Q&A

Tags: Scambait Village | Creator Event/Activity

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 208 (Scambait Village) - [Map](#)

Description:

Drop-in Q&A running throughout the village whenever the hall is open. Knowledgeable volunteers are stationed across the booth and can answer questions about scambaiting techniques, tools, safety, community norms, legal considerations, and anything else related to fighting scammers. No session times, no signup. Come by whenever, ask whatever. Casual and welcoming for both newcomers and veterans. Note that Q&A pauses briefly during scheduled talks and sessions at the village, listed separately on this schedule.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Scambait Village - Sunday - 10:00-15:59 PDT

Title: Open Q&A

Tags: Scambait Village | Creator Event/Activity

When: Sunday, Aug 9, 10:00 - 15:59 PDT

Where: LVCCW Level 1 Hall 1 208 (Scambait Village) - [Map](#)

Description:

Drop-in Q&A running throughout the village whenever the hall is open. Knowledgeable volunteers are stationed across the booth and can answer questions about scambaiting techniques, tools, safety, community norms, legal considerations, and anything else related to fighting scammers. No session times, no signup. Come by whenever, ask whatever. Casual and welcoming for both newcomers and veterans. Note that Q&A pauses briefly during scheduled talks and sessions at the village, listed separately on this schedule.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Opening Panel - "Is Red Teaming Dead?"

Tags: Red Team Village | Misc

When: Friday, Aug 7, 10:00 - 10:59 PDT

Where: LVCCW Level 1 Hall 1 309 (Red Team Village) Workshop Stage 1 - [Map](#)

Description:

Moderated By Ben Sadeghipour (@NahamSec) Guests: Ads Dawson (0xmoose) Ryan Montgomery (@0day) Billy Giles

Speakers: Ads Dawson, Ben "NahamSec" Sadeghipour, Billy Giles, Ryan Montgomery

SpeakerBio: Ads Dawson, Staff AI Security Researcher, OWASP GenAI Security Project founder

Ads Dawson founded the OWASP GenAI Security Project and led it to flagship status — the fastest in OWASP history. As a Staff AI Security Researcher at Dreadnode, he specializes in exploiting ML and AI systems, harnessing AI for offensive cybersecurity through capability development and exploit development, and conducting red team operations against frontier models for government, military, and tier-1 labs. He is lead author of AIRTBench (arXiv), the first benchmark for autonomous AI red teaming in LLMs, and author of AI Native LLM Security (Packt, 2025).

A senior red team operator with BT6 (the frontier AI red team), ranked #2 in Canada on HackerOne (2025/2026), and selected for Meta's MBBRC live hacking event, Ads is a HackerOne US South Ambassador, BugCrowd Hacker Advisory Board member, MITRE AI Working Group contributor, and leads the OWASP Toronto chapter. He spoke at Bug Bounty Village DC33 on the BT6 AI jailbreaking panel and is also presenting "Exfil Everything: A Year of Stealing Data from AI Agents" at Bug Bounty Village DC34 (schedule pending publication).

SpeakerBio: Ben "NahamSec" Sadeghipour

Ben Sadeghipour (NahamSec) is a security researcher, ethical hacker, and educator who has spent more than a decade finding and disclosing critical vulnerabilities in some of the world's largest organizations. As one of the most recognized names in the bug bounty community, he has reported thousands of security flaws and consistently ranked among the top researchers on leading hacking platforms. Beyond his own research, Ben is passionate about lowering the barrier to entry in cybersecurity. Through his widely followed educational content, live streams, and the conferences he founds and organizes, he has helped train a new generation of hackers around the world. His work blends deep technical expertise with a commitment to mentorship and community building. Ben speaks regularly at industry conferences on offensive security, bug bounty hunting, and building a career in cybersecurity.

SpeakerBio: Billy Giles

Billy Giles is an Offensive Security leader and practitioner who specializes in red/purple teaming and network penetration testing. With a deep passion for understanding adversary behaviors, he helps organizations across a multitude of industries assess their security postures, identify and remediate vulnerabilities, and build stronger defenses by thinking like an attacker.

Billy is also the creator of Thinking Offensively. Through this project he examines offensive security strategy topics to help cybersecurity leaders anticipate threats and inform decision making, while also providing tools, playbooks, and techniques that red teams can apply directly to their work. His mission is to bridge strategy and execution to help organizations think offensively and stay ahead of evolving threats.

SpeakerBio: Ryan Montgomery

No BIO available



Cloud Village - Friday - 10:00-10:10 PDT

Title: Opening Talk

Tags: Cloud Village | Creator Talk/Panel

When: Friday, Aug 7, 10:00 - 10:10 PDT

Where: LVCCW Level 3 W313 (Cloud Village Talks) - [Map](#)

Description:

SpeakerBio: Jayesh Singh Chauhan

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Maker's Village - Saturday - 14:15-14:45 PDT

Title: Operation Restoration

Tags: Maker's Village | Creator Event/Activity

When: Saturday, Aug 8, 14:15 - 14:45 PDT

Where: LVCCW Level 1 Hall 1 301 (Makers' Village) - [Map](#)

Description:

Every forgotten machine has a story—and a second chance. This talk explores the multidisciplinary maker ethos through restoration: where machining, woodworking, sewing, CAD, 3D printing, and whatever other skills you have in your toolbox come together to resurrect forgotten machines and breathe new life into once-loved objects.

SpeakerBio: Cannibal

No BIO available

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Social Gatherings/Events - Thursday - 18:00-19:59 PDT

Title: Operator, Please Hold - DCG Social

Tags: Party | DEF CON Groups

When: Thursday, Aug 6, 18:00 - 19:59 PDT

Where: LVCCW Level 2 W238 (DEF CON Groups) - [Map](#)

Description:

Operator, Please Hold is the official DEF CON Groups party at DEF CON 34 - a social for hackers, DCG organizers, and community builders from around the world.

This is where DEF CON Groups converge off the mailing lists and out of Discord. Expect familiar faces, new connections, and conversations that jump from local meetups to global chaos in about five minutes. No talks. No agenda. Just hackers who actually show up for their communities, in one room, at the same time.

Whether you run a group, help keep one alive, or are looking to plug into your local hacker scene, this is your stop. Come say hi, compare notes, and meet the humans behind the handles.

Operator, please hold. Your people are on the line.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: OSINT for Hackers Redux

Tags: Red Team Village | Misc

When: Saturday, Aug 8, 16:00 - 16:59 PDT

Where: LVCCW Level 1 Hall 1 309 (Red Team Village) Workshop Stage 2 - [Map](#)

Description:

In this Workshop and Tactic, attendees will be exposed to and get hands-on with some of the most impactful strategies, techniques, and tools to increase the value of OSINT to their red-teaming activities. As a guided learning experience, the instructors will immerse attendees in the topic and provide numerous hands-on opportunities within just the Workshop component. In addition, the dedicated Tactic (which will be offered multiple times) will focus on building secure sock puppets (fake identities) for use in the recon and information gathering phases of red team and penetration testing operations.

Speakers: Lee McWhorter, Sandra Stibbards

SpeakerBio: Lee McWhorter

Lee McWhorter, Owner & Chief Geek at McWhorter Technologies, has been involved in IT since his early days and has over 30 years of experience. He is a highly sought after professional who first learned about identifying weaknesses in computer networks, systems, and software when Internet access was achieved using a modem. Lee holds an MBA and more than 20 industry certifications in such areas as System Admin, Networking, Programming, Linux, IoT, and Cybersecurity. His roles have ranged from the server room to the board room, and he has taught for numerous universities, commercial trainers, and nonprofits. Lee is the SWAG Master and a Core Staff member for the Red Team Village at DEFCON; and works closely with the Pacific Hackers Association, Dark Arts Village at RSAC, Texas Cyber Summit, CompTIA, and the CompTIA Instructor Network as a Speaker, SME, and Instructor.

SpeakerBio: Sandra Stibbards

Sandra Stibbards opened her investigation agency, Camelot Investigations, in 1996. Currently, she maintains a private investigator license in the state of California. Sandra specializes in financial fraud investigations, competitive intelligence, counterintelligence, business and corporate espionage, physical penetration tests, online vulnerability assessments, brand protection/IP investigations, corporate due diligence, and Internet investigations. Sandra has conducted investigations internationally in five continents and clients include several Fortune 500 and international companies. Sandra has been providing training seminars and presentations on Open Source Intelligence (OSINT) internationally since 2010 to federal governments and corporations.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: OSINT Is Still a Thinking Game: Surviving AI Without Losing Tradecraft

Tags: Recon Village | Creator Talk/Panel

When: Friday, Aug 7, 13:00 - 13:45 PDT

Where: LVCCW Level 1 Hall 3 801 (Creator Stage 2) - [Map](#)

Description:

The OSINT landscape is undergoing a fundamental shift. Artificial Intelligence is no longer just a tool; it is becoming a crutch. As analysts increasingly rely on LLMs to triage data, translate foreign slang, and summarize massive datasets, a dangerous cognitive atrophy is taking hold. We are trading the slow, deliberate friction of critical thinking for the illusion of speed and certainty.

This talk, "OSINT Is Still a Thinking Game," exposes the hidden vulnerabilities of AI dependence in intelligence work. Through real-world case studies—from misinterpreting Telegram chatter to falsely flagging logistics data—we will examine how the "Good Enough" trap leads to catastrophic analytical failures.

More importantly, this session provides a concrete defense framework. Attendees will learn the four essential habits required to survive the AI era: reading the raw source, forcing a second hypothesis, separating speed from confidence, and auditing dependence. The tools will inevitably get better, but the thinking must get sharper. Join this session to learn how to maintain your tradecraft, keep your judgment visible, and ensure that in the age of automation, defensibility always wins over speed.

SpeakerBio: Nico Dekens, Dutch_OSINTGUY SVP of Engineering & Chief Innovator @ Shadowdragon.io

Nico Dekens is the owner of Dutch Osint Guy Intelligence Services and an All Source Analyst who specializes in Open Source Intelligence (OSINT), online Human Intelligence (HUMINT) and Online investigations. Nico eats, sleeps, and lives everything which has to do with OSINT, online investigations, intelligence gathering and analysis. He has over 20 years' experience as an (all source) Intelligence Analyst in Dutch Law Enforcement. There, he analyzed murder cases, international narcotics cases, stolen art cases, gang violence cases, political disturbance cases. Investigated and analyzed online jihadist groups & conducted several online covert virtual HUMINT investigations.

“

Known online as @Dutch_OsintGuy, Nico is very active within the OSINT community. As the owner of Dutch Osint Guy Intelligence Services, Nico provides consultancy and training for Open-Source Intelligence (OSINT), risk assessments, keynotes, security awareness, and implementation of structured team methodologies. He is also a co-founder of the OSINTCurio.us project.

“

Nico chose to be an OSINT Specialist and Cyber Intelligence Analyst because he wanted to help to make the world a safer place and because OSINT is one of the fastest fields in the cyber realm, with an ever-changing landscape. This helps him to remain in a constant state of learning and giving back what he's learned to others who also want to make this (digital) world a safer place.

“

Before he became a SANS instructor, Nico helped set up the OSINT units within the Dutch Government as well as train and educate thousands of government employees on how to work in structured teams and perform excellent online investigations.

“

Nico is a SANS Instructor for SEC497 Practical Open-Source Intelligence (OSINT) and lead author of SEC587: Advanced Open-Source Intelligence (OSINT) Gathering and Analysis. As an instructor, he uses practical real-world examples as much as possible. “Being an instructor isn’t one-way traffic; it is a dynamic process between the student and instructor” Nico says. He is also a faculty member of the SANS Technology Institute, an NSA Center of Academic Excellence in Cyber Defense and multiple winner of the National Cyber League competition.

With all his OSINT and intelligence gathering and analysis experience that he brings to the table, Nico is able to share his unique experiences with his students on Open-Source Intelligence.

“

Among his biggest career highlights, he is proud of helping to stop terrorists from executing their attacks and stopping child predators. It’s his goal to keep the world safe and help those who are not able to defend themselves. Nico has had students come back to him years later, thanking him for techniques he taught them that played a role in their investigations.

“

Nico has been honored by Head of Europol, the DHS, and NATO for his efforts in the OSINT field. He’s received a letter of gratitude from the Dutch Military Cyber Intelligence and Cyber Defense department. He’s also been honored by Dutch Law Enforcement for his efforts in counter terrorism and online investigations.

“

Nico holds certifications as a Police Detective, Operational Intelligence Analyst, Tactical Intelligence Analyst, Strategical Intelligence Analyst, Open-Source Intelligence Analyst, Cyber Intelligence Tradecraft Professional, Online Counter Terrorism Specialist.

“

Nico is the 2023 Open Source Intelligence Champion of the Year, presented by the OSMOSIS Institute.

Nico is a typical gadget nerd. When he’s not teaching, he likes to play around and test new gadgets that are closely related to the cyber field. So Raspberry pi, esp8266, esp32, microbits, iot devices are things he likes to learn more about. He also likes to work-out and play basketball. He’s also a collector of unique sneakers.

Currently Nico is working as Senior Vice President of Engineering & Chief Innovator at ShadowDragon.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

OSINT For Good Community - Saturday - 16:00-16:59 PDT

Title: OSINT Search party CTF Debrief

Tags: OSINT For Good Community | Creator Workshop

When: Saturday, Aug 8, 16:00 - 16:59 PDT

Where: LVCCW Level 1 Hall 4 1307 (OSINT4Good Community) - [Map](#)

Description:

An opportunity to ask questions and get clarification on things that happened during the CTF.

SpeakerBio: Trace Labs Staff

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

OSINT For Good Community - Saturday - 17:00-17:15 PDT

Title: OSINT Search Party CTF Prize and Award Announcements.

Tags: OSINT For Good Community | Creator Event/Activity

When: Saturday, Aug 8, 17:00 - 17:15 PDT

Where: LVCCW Level 1 Hall 4 1307 (OSINT4Good Community) - [Map](#)

Description:

Prizes and awards from the Goba OSINT Search Party CTF will be announced.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Noob Community - Friday - 13:30-13:59 PDT

Title: OSINT: Zero To Hero

Tags: Noob Community | Creator Talk/Panel

When: Friday, Aug 7, 13:30 - 13:59 PDT

Where: LVCCW Level 1 Hall 4 1417 (Noob Community) - [Map](#)

Description:

If you're curious on how this field has evolved, I'll take you on a journey from beginner to extremely advanced level intelligence, all using a computer. I'll demo techniques live and answer questions like: How has OSINT evolved over the years? What powers do you get from developing this skill?

SpeakerBio: Mishaal Khan

No BIO available

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

OSINT For Good Community - Sunday - 10:00-13:59 PDT

Title: OSINT4Good Community - DC NextGen Content

Tags: OSINT For Good Community | Creator Event/Activity

When: Sunday, Aug 9, 10:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 4 1307 (OSINT4Good Community) - [Map](#)

Description:

Make this a stop on your DC NextGen journey, solve the challenge, and earn a digital badge!

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

OSINT For Good Community - Friday - 10:00-17:59 PDT

Title: OSINT4Good Community - DC NextGen Content

Tags: OSINT For Good Community | Creator Event/Activity

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 4 1307 (OSINT4Good Community) - [Map](#)

Description:

Make this a stop on your DC NextGen journey, solve the challenge, and earn a digital badge!

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

OSINT For Good Community - Saturday - 10:00-17:59 PDT

Title: OSINT4Good Community - DC NextGen Content

Tags: OSINT For Good Community | Creator Event/Activity

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 4 1307 (OSINT4Good Community) - [Map](#)

Description:

Make this a stop on your DC NextGen journey, solve the challenge, and earn a digital badge!

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

OSINT For Good Community - Saturday - 17:15-17:59 PDT

Title: OSINT4Good Sticker Swap

Tags: OSINT For Good Community | Creator Event/Activity

When: Saturday, Aug 8, 17:15 - 17:59 PDT

Where: LVCCW Level 1 Hall 4 1307 (OSINT4Good Community) - [Map](#)

Description:

Bring some stickers, take some stickers. There will be some specially themed OSINT4Good stickers available only here!



[Return to Index](#) - Add to Google

- ics [Calendar](#) file

Title: OSINT4Good: What it takes to find missing people

Tags: OSINT For Good Community | Creator Talk/Panel

When: Friday, Aug 7, 10:00 - 10:59 PDT

Where: LVCCW Level 1 Hall 3 1100 (Creator Stage 7) - [Map](#)

Description:

Have you ever wondered what it takes to use gamified OSINT to find missing people? Moderated by a Director from Trace Labs, this panel brings together a participant (who won Most Valuable OSINT), a coach (who has coached more times than anyone on the planet), and a report writer (who leads the team of report writers) to walk you through the different perspectives of this work.

Speakers: Angela Ramos, Kenny J, Brent Louie

SpeakerBio: Angela Ramos, University of Tampa

Angela Ramos is a University of Tampa cybersecurity lecturer. She leads the Scam Busters student program, coaches Trace Labs Search Party CTFs, and volunteers with US Cyber Games. She holds the GCIH, GSLC, and CEH certifications and spent a decade in DoD cyber operations.

SpeakerBio: Kenny J, Trace Labs

Senior Infrastructure Engineer by day. Osint for Good by night. His is the only Trace Labs coach to have coached 20+ CTFs, earning him the singular rank of Legendary Coach.

SpeakerBio: Brent Louie, Reporting Team Lead at Trace Labs

Brent Louie is the Reporting Team Lead at Trace Labs and an Associate Director of Data Science with more than 15 years of experience in the biotechnology industry. He focuses on applying OSINT methodologies to missing persons investigations and helping transform crowdsourced research into actionable investigative leads for law enforcement.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: OT Round table. Real talk on how to protect your OT spaces

Tags: ICS Village | Creator Talk/Panel

When: Saturday, Aug 8, 14:00 - 14:45 PDT

Where: LVCCW Level 1 Hall 3 801 (Creator Stage 1) - [Map](#)

Description:

A hosted open discussion on strategies for protecting OT with Tom Van Norman and Dillon Lee.

Speakers: Aaron Crow, Tom VanNorman, Dillon Lee

SpeakerBio: Aaron Crow, PrOTect IT All

Aaron is the host of the #2 OT Security Podcast "PrOTect IT All". Aaron has spent the last decade helping asset owners across utilities, manufacturing, food and beverage, and transportation build OT cybersecurity programs that actually hold up in operational reality, not just on a compliance checklist. Today he is the Senior Director at Arcova (formerly MorganFranklin Cyber), leading OT/ICS engagements: assessments, SOC design, NERC CIP, segmentation architecture, and Cyber-Informed Engineering. Before this he was CTO of Industrial Defender, and spent 4+ years at EY running an OT program that included a 3,000-site deployment at a major North American power utility. His podcast, PrOTect IT (100+ episodes, Top Rated by Feedspot in Industrial Security) has featured guests including Mike Holcomb, Sean Tufts, Thomas VanNorman, Jori VanAntwerp, Bryson Bort, Clint Bodungen, and many others. He is a long-time volunteer with ICS Village.

SpeakerBio: Tom VanNorman

Tom VanNorman is the co-founded ICS Village and leads the CyPhy Product group at GRIMM, where his primary focus is securing Industrial Control Systems and the networking of such systems. Tom brings an unparalleled level of operational knowledge and experience — he has been working in is the Operational Technology (OT) field for almost three decades. He has considerable expertise in constructing Cyber-Physical testing environments for OT systems.

Retired from the Air National Guard after over 20 years of service, where he worked in Cyber Warfare Operations.

SpeakerBio: Dillon Lee, Dragos, Inc

Dillon volunteers for ICS Village and works at Dragos as a Principal Technical Account Manager. Throughout the year he volunteers for ICS Village to increase public's awareness of the need OT systems have for cybersecurity with interactive learning like CTF, TTX, and interactive demos. As a Technical Account manager, he is a specialized product expert who works collaboratively with OT/IT organizations to strategically plan for successful deployments and help realize optimizations of their OT processes.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: OT Segmentation Under Operational Constraints

Tags: ICS Village | Creator Talk/Panel

When: Friday, Aug 7, 15:00 - 15:30 PDT

Where: LVCCW Level 1 Hall 3 801 (Creator Stage 1) - [Map](#)

Description:

OT network segmentation projects rarely fail because of missing firewall features or lack of security tooling. They fail because industrial environments operate under constraints that traditional IT security programs do not fully account for: limited maintenance windows, fragile legacy systems, vendor-controlled architectures, operational distrust of change, and the reality that reliability and uptime often outweigh security priorities during production events.

This presentation focuses on the operational side of OT segmentation: how industrial organizations actually plan, prioritize, communicate, implement, and sustain segmentation initiatives in production environments. Rather than treating segmentation purely as a technical firewall exercise, the session examines segmentation as an operational optimization problem balancing security risk, operational disruption, safety requirements, maintenance constraints, compliance pressure, and organizational ownership. Topics discussed include:

Phased rollout strategies and pilot deployments
Change validation and rollback planning
Segmentation drift and long-term erosion of controls
Vendor and integrator access throughout project lifecycles
Operational trust-building through monitor-first deployments and packet-capture-driven validation

We will explore why many environments gradually return to flat networks despite significant investment in segmentation initiatives. Real-world examples from utility and critical infrastructure environments will demonstrate how operational realities, maintenance pressure, and organizational ownership challenges frequently undermine otherwise well-designed security architectures.

Attendees will leave with practical guidance for approaching OT segmentation as an operational change-management problem rather than simply a firewall deployment exercise, along with implementation patterns that improve security posture without creating unnecessary operational disruption.

SpeakerBio: Tony Turner

Tony is a security architect with over 30 years of experience across IT and operational technology (OT) environments. As VP of Product at Frenos, he leads the development of a simulated OT penetration testing platform that uses digital twin modeling and adversary-driven analysis to evaluate real-world risk in industrial systems.

His background is grounded in decades as an asset owner, including critical infrastructure protection at a major U.S. airport, incident command for state public health systems, disaster recovery engineering for hurricane response, and security programs across electric power and global semiconductor manufacturing. This operational experience informs a practical, systems-driven approach to cybersecurity that prioritizes real impact over theoretical risk.

Tony's work focuses on how attackers actually operate in complex environments, spanning network reachability, adversary actions, supply chain risk, and software provenance. He is the author of Software Transparency and creator of the SANS SEC547 course Defending Product Supply Chains. He has presented at S4 Conference and other industry forums on topics including threat modeling with BOMs and the real-world effectiveness of industrial firewall DPI.

He actively contributes to research efforts with organizations such as MITRE, Idaho National Laboratory, CISA, and ISA, particularly in advancing Cyber Informed Engineering (CIE). He also leads defendics.org, a nonprofit focused on improving foundational OT security practices for resource-constrained asset owners.



Title: Ouroboros Attack! Recursive AI-Assisted 0-Day Hunting

Tags: Red Team Village | Misc

When: Saturday, Aug 8, 12:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 1 309 (Red Team Village) Tactic Table 1 - [Map](#)

Description:

This session presents a practical workflow for discovering and building real zero-day vulnerabilities using a recursive AI-assisted approach. The first part of the talk examines a logic flaw identified in the rendering mechanism of a large language model environment. Through structured interaction and controlled prompt chaining, inconsistencies in rendering state handling were exposed. By refining responses and feeding outputs back into follow-up prompts, the system revealed weaknesses in its own internal logic. Under specific crafted conditions, this behavior demonstrated a scenario that could lead to sensitive data exposure, including API-related material.

The second part of the session applies the same structured workflow to traditional web applications: SquirrelMail , ISPCConfig , DokuWiki. Using recursive hypothesis refinement, attack surface expansion, and manual validation, multiple high and critical impact zero-day vulnerabilities were identified and confirmed with working proof-of-concept exploit chains.

These vulnerabilities have not yet been publicly disclosed. The conference presentation will include their first public technical analysis and exploit breakdown.

The focus of the talk is methodology: How to structure AI interaction for vulnerability research How recursive prompt chaining expands edge-case discovery How model output can be converted into real exploit paths Where manual validation remains necessary

This is a technical session centered on real exploit development and practical offensive research.

Speakers: Mehmet Önder Key, Temel Demir

SpeakerBio: Mehmet Önder Key, Cyber Security Consultant

Önder Key is a cybersecurity consultant specializing in critical infrastructure security, zero-day vulnerability analysis, and offensive security. He has advised organizations in high-security sectors such as defense, aerospace, and finance, with hands-on experience in both red teaming and strategic security engineering. His work has been featured across numerous countries and platforms, contributing to the discovery of systemic vulnerabilities. Currently, he provides consultancy to TurkNet and continues to advance the global offensive security ecosystem by challenging traditional approaches to cybersecurity.

SpeakerBio: Temel Demir

Temel Demir is a cybersecurity researcher and hardware architect specializing in hardware defense, offensive security, and the protection of critical infrastructure. With a core focus on embedded system vulnerabilities and Layer-1/Layer-2 network manipulation, his research involves developing deterministic, hardware-enforced frameworks that bypass traditional software-defined security flaws. Having previously shared security research on global stages, his work bridges the gap between sophisticated threat actor methodologies and immutable physical security barriers.

Title: Overcast: Video OSINT Agent. Point It at 100 Videos, Ask Anything

Tags: Intro/Beginner | AI | DEF CON Demo Labs | Offense/Red Team | Threat Intel/Hunting | DEF CON Demo Labs

When: Saturday, Aug 8, 16:00 - 16:45 PDT

Where: LVCCW Level 1 Hall 3 902 (Demo Labs Track 6) - [Map](#)

Description:

Conference talks, earnings calls, product demos, training videos. Organizations put hours of footage online every week, full of things they didn't mean to share: hostnames in terminal windows, org charts on slides, infrastructure details dropped during Q&A. Traditional OSINT can't touch video at scale, and manual review falls apart past a handful of recordings.

Overcast is a CLI agent and skill pack for video OSINT that drops into any agentic harness, such as Claude Code, Codex, or Tyncloud, giving it senses plus recon and targeting reach, organized around an investigation case. Point it at 10 videos or 1,000 and it turns footage into cited evidence: speech, video understanding, on-screen text and objects, faces, and named entities, all accumulating in persistent case memory.

Discovery runs on the same case: scan and monitor sweep sources and surface reviewable findings. Ask across the whole corpus and get answers cited to the exact record and timestamp, backed by tiered retrieval. Match a photo against thousands of clips to find a person. Each subcommand is modular and pluggable, so analysts can drop one into other agent flows, author custom skills, or feed Overcast's media analysis into existing recon and security tooling to complete the mission.

SpeakerBio: Kevin "kdrwins" Dela Rosa

Kevin Dela Rosa is a multimodal AI researcher and engineer with 17+ years in computer vision, NLU, and large-scale retrieval. He led engineering teams at Snapchat building billion-scale visual search and generative AI products, worked on large-scale ML at Amazon, and interned at NIST and SPAWAR on NLP and information retrieval for government applications. He's published at ACM WWW, ACM CAIS, IEEE ICCV, KDD, CVPR, NeurIPS, AAAI, and ISMIR, and has spoken at AWS re:Invent, KubeCon, and CascadiaJS. He's currently CTO of Cloudglue, where he builds video understanding infrastructure.

At DEF CON 33 he presented "Autonomous Video Hunter" at Recon Village, demoing an AI agent that investigated video corpora using face recognition, logo detection, and content analysis to produce structured OSINT reports. Overcast is the evolution of that work: a CLI agent and skill pack that gives any agentic harness senses plus recon and targeting reach, organized around an investigation case with persistent memory, cited evidence, and modular subcommands that plug into other recon and security workflows.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Overcast: Video OSINT Agent. Point It at 100 Videos, Ask Anything

Tags: Intro/Beginner | AI | DEF CON Demo Labs | Offense/Red Team | Threat Intel/Hunting | DEF CON Demo Labs

When: Friday, Aug 7, 12:00 - 12:45 PDT

Where: LVCCW Level 1 Hall 3 902 (Demo Labs Track 6) - [Map](#)

Description:

Conference talks, earnings calls, product demos, training videos. Organizations put hours of footage online every week, full of things they didn't mean to share: hostnames in terminal windows, org charts on slides, infrastructure details dropped during Q&A. Traditional OSINT can't touch video at scale, and manual review falls apart past a handful of recordings.

Overcast is a CLI agent and skill pack for video OSINT that drops into any agentic harness, such as Claude Code, Codex, or Tyncloud, giving it senses plus recon and targeting reach, organized around an investigation case. Point it at 10 videos or 1,000 and it turns footage into cited evidence: speech, video understanding, on-screen text and objects, faces, and named entities, all accumulating in persistent case memory.

Discovery runs on the same case: scan and monitor sweep sources and surface reviewable findings. Ask across the whole corpus and get answers cited to the exact record and timestamp, backed by tiered retrieval. Match a photo against thousands of clips to find a person. Each subcommand is modular and pluggable, so analysts can drop one into other agent flows, author custom skills, or feed Overcast's media analysis into existing recon and security tooling to complete the mission.

SpeakerBio: Kevin "kdrwins" Dela Rosa

Kevin Dela Rosa is a multimodal AI researcher and engineer with 17+ years in computer vision, NLU, and large-scale retrieval. He led engineering teams at Snapchat building billion-scale visual search and generative AI products, worked on large-scale ML at Amazon, and interned at NIST and SPAWAR on NLP and information retrieval for government applications. He's published at ACM WWW, ACM CAIS, IEEE ICCV, KDD, CVPR, NeurIPS, AAAI, and ISMIR, and has spoken at AWS re:Invent, KubeCon, and CascadiaJS. He's currently CTO of Cloudglue, where he builds video understanding infrastructure.

At DEF CON 33 he presented "Autonomous Video Hunter" at Recon Village, demoing an AI agent that investigated video corpora using face recognition, logo detection, and content analysis to produce structured OSINT reports. Overcast is the evolution of that work: a CLI agent and skill pack that gives any agentic harness senses plus recon and targeting reach, organized around an investigation case with persistent memory, cited evidence, and modular subcommands that plug into other recon and security workflows.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: OWASP AIBOM Generator

Tags: AppSec Village | Creator Event/Activity | All Audiences

When: Saturday, Aug 8, 14:00 - 14:59 PDT

Where: LVCCW Level 1 Hall 2 604 (Appsec Village) Arsenal - [Map](#)

Description:

AI systems increasingly depend on opaque model, dataset, and tooling supply chains, but most teams still lack a practical way to capture what is inside them. This Arsenal session demonstrates the OWASP AIBOM Generator, an open-source tool from the OWASP GenAI Security Project that creates CycloneDX-based AI Bills of Materials (AIBOM) for AI/ML assets.

Attendees will see how to generate AIBOMs that can support AI transparency, security review, governance, incident response, and software supply chain risk management without turning the process into a manual documentation review exercise.

Speakers: Dmitry Raidman, Helen Oakley

SpeakerBio: Dmitry Raidman

Dmitry Raidman is the Co-Founder and CTO of CyBeats, where he leads product and technology strategy focused on software supply chain security, SBOM management, and product security compliance. He works with organizations across regulated industries to operationalize SBOMs, improve software transparency, and manage vulnerability and third-party component risk at scale.

Dmitry is also active in the cybersecurity community, contributing to initiatives around AI security, SBOM adoption, and software supply chain risk. He is involved with the OWASP GenAI Security Project and the AIBOM Initiative, helping advance practical approaches for documenting and managing AI-related software and model supply chain exposure.

His work focuses on helping organizations move beyond checklist compliance toward measurable product security capabilities, continuous visibility, and faster response to emerging software and supply chain threats.

SpeakerBio: Helen Oakley

Helen Oakley, CISSP, GPCS, GSTRT, works at the intersection of AI, cybersecurity, and software supply chains—where the rules are still being written. At SAP, she leads a global team of architects, security experts, and scientists, securing development and pipelines at scale. Helen is part of the core leadership team of the OWASP GenAI Security Project and co-leads initiatives on AIBOM and Agentic Security, contributes into industry papers like Agentic AI Threats & Mitigations Guide, OWASP Top 10 for Agentic Apps, and more. Helen has co-led AIBOM efforts with CISA, and is the original creator of the OWASP FinBot CTF and the first open-source OWASP AIBOM Generator for Hugging Face models. Named one of the Top 20 Canadian Women in Cybersecurity, she co-founded LeadingCyberLadies.com to support the next wave of builders, breakers, and leaders.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: OWASP Amass v5.0

Tags: OWASP Foundation | Creator Workshop

When: Friday, Aug 7, 16:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 4 1415 (OWASP Foundation) - [Map](#)

Description:

The OWASP Amass Project has become a foundational toolset for security researchers, bug bounty hunters, red teamers, and defenders who rely on automated reconnaissance and external asset discovery to map attack surfaces. With the release of Amass v5.0, the project has undergone a major architectural transformation centered around the Open Asset Model (OAM)—a structured property graph that defines how Internet-facing assets and their relationships are stored, analyzed, and queried.

This two-hour hands-on workshop, led by Jeff Foley, the project's founder and long-time maintainer, offers attendees a first look at Amass v5.0's new intelligence collection engine, which seamlessly populates the Open Asset Model database during enumeration operations. The session will walk through how Amass collects and organizes OSINT from various sources—including DNS records, WHOIS/RDAP data, TLS certificates, and more—and models the results as a dynamic graph of properties and relationships between discovered assets.

Participants will learn to use core Amass tools such as:

amass enum – for deep, recursive asset discovery using passive and active techniques

amass subs – for quick subdomain discovery from the Open Asset Model database

amass viz – to render interactive visualizations of asset relationships in the Open Asset Model

In addition to these staples, the workshop will introduce the new assoc tool, a powerful query interface designed to unlock the true potential of the Open Asset Model database. Built around a custom Triples query language, the assoc tool enables users to describe paths—called association walks—through the asset graph, surfacing linked insights across related properties (e.g., domains associated with a network, IPs linked to DNS records, etc.). The language is inspired by RDF-style triples but optimized for simplicity and clarity in cybersecurity investigations.

Amass v5.0 also ships with completely refactored documentation, providing diagrams to help users understand the data types, their fields, and their associations within the OAM. This new documentation dramatically lowers the learning curve for users new to the Amass Project, making it easier to build mental models of how different types of Internet assets are discovered and interrelated.

This workshop will include a live walkthrough of setting up and running Amass v5.0, from enumeration to advanced queries. Participants will leave with hands-on experience using the full Amass suite, understanding how the Open Asset Model works under the hood, and writing association walk queries using Triples.

What to Expect:

Real-world reconnaissance examples using Amass against publicly available targets

Query design exercises with assoc to extract actionable intelligence

Tips for integrating Amass data into your own tooling and pipelines

Visual mapping of organizational assets using OAM and viz

Level: Intermediate Some experience with OSINT tools, command-line interfaces, or network security is recommended but not required. The workshop is designed to be self-contained and accessible.

Attendees are encouraged to bring a laptop and follow along. Project contributors will be present throughout the session to provide hands-on support, answer questions, and help troubleshoot issues in real time, making this a highly interactive experience.

By the end of the session, participants will walk away with practical skills in reconnaissance, data extraction from structured asset models, and a solid understanding of how Amass v5.0 is redefining modern Internet-wide discovery.

Join us at DEF CON to explore the future of OSINT automation and asset intelligence with OWASP Amass!

SpeakerBio: Jeff Foley, Founder and Project Leader at OWASP Amass Project

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: OWASP Chapter Meetup

Tags: OWASP Foundation | Creator Event/Activity

When: Sunday, Aug 9, 11:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 4 1415 (OWASP Foundation) - [Map](#)

Description:

This one's for the chapter leads, the regulars, the new folks, and everyone who makes OWASP what it is. Join us at DEFCON 33 for a meetup made to foster connection between OWASP chapters. It's a chance to share wins, swap challenges, build relationships, and spark ideas that reach beyond our local scenes. Whether you're repping your city or just curious about how others are building community, pull up. The global OWASP family is real—and this is where we get to feel it.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Contests - Friday - 10:30-11:30 PDT

Title: OWASP CTF: Getting started & welcome

Tags: OWASP Foundation | OWASP Foundation CTF | Contest

When: Friday, Aug 7, 10:30 - 11:30 PDT

Where: LVCCW Level 1 Hall 4 1415 (OWASP Foundation) - [Map](#)

Description:

New to CTFs or application security? Join us before the competition for an introductory session designed to help newcomers get up to speed. We'll walk through the challenge format, the secure development lifecycle it simulates, and the tools and techniques you'll use - from finding vulnerabilities and implementing secure fixes to leveraging OWASP open source tooling and AI-assisted security workflows. Whether you're brand new or just looking for a refresher, this session will help you feel prepared and confident before the CTF begins.

Speakers: Diego Cotel, Chris "dafinga" Maenner, Christian "DeadlyFluVirus" Nuss

SpeakerBio: Diego Cotel, Staff Cloud & Security Engineer

I'm a cloud and security engineer working at the intersection of infrastructure and security. I harden AWS, Kubernetes, and GitOps pipelines, and build tooling that surfaces misconfigurations, drift, and blast radius before an attacker finds them first. I treat security as an architecture problem, not a checklist — breaking systems to understand them, then designing secure-by-default platforms. I write about offensive and defensive cloud security at [dcotel.dev](#).

SpeakerBio: Chris "dafinga" Maenner, Board Member at BSides Philadelphia

Chris Maenner is the founder of Palmtree Ventures, where he spends his time securing AI systems, Kubernetes, cloud platforms, and developer tooling without getting in the way of shipping software. Over the last 15+ years, he's worked across startups and Fortune 50 companies building product, platform, and cloud security programs. When he's not doing his day job, Chris helps build CTFs and security projects for DEF CON's Blue Team Village and OWASP, including leading engineering efforts around Project Obsidian. He also serves on the board of BSides Philadelphia, contributes to the OWASP Secure Agent Playbook, and regularly speaks about AI security, Kubernetes, cloud-native security, and the lessons learned from actually trying to secure this stuff in production.

SpeakerBio: Christian "DeadlyFluVirus" Nuss, Scaffoldly

Full-stack development; Multi-cloud architecture, security and reliability; Automation enthusiast; Tech team development and leadership; Entrepreneur; Founder of Scaffoldly

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Contests - Saturday - 10:00-17:59 PDT

Title: OWASP CTF

Tags: OWASP Foundation | OWASP Foundation CTF | Contest

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 4 1415 (OWASP Foundation) - [Map](#)

Description:

This challenge simulates a real-world secure development lifecycle, where security professionals must not only identify vulnerabilities but also collaborate with development teams to implement, validate, and deploy secure fixes.

By completing the challenge, participants gain hands-on experience in:

- Web application exploitation
- Secure coding and vulnerability remediation
- Open-source security tooling from the OWASP ecosystem
- Responsible disclosure and patch submission workflows
- Using AI tools to assist in vulnerability analysis and remediation

The ultimate goal is to help practitioners develop the full skill set required to identify vulnerabilities, implement secure fixes, and deploy those fixes safely within their infrastructure.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Contests - Friday - 10:00-17:59 PDT

Title: OWASP CTF

Tags: OWASP Foundation | OWASP Foundation CTF | Contest

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 4 1415 (OWASP Foundation) - [Map](#)

Description:

This challenge simulates a real-world secure development lifecycle, where security professionals must not only identify vulnerabilities but also collaborate with development teams to implement, validate, and deploy secure fixes.

By completing the challenge, participants gain hands-on experience in:

- Web application exploitation
- Secure coding and vulnerability remediation
- Open-source security tooling from the OWASP ecosystem
- Responsible disclosure and patch submission workflows
- Using AI tools to assist in vulnerability analysis and remediation

The ultimate goal is to help practitioners develop the full skill set required to identify vulnerabilities, implement secure fixes, and deploy those fixes safely within their infrastructure.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: OWASP FinBot CTF: Hands-On Agentic AI Threats

Tags: AppSec Village | Creator Event/Activity | All Audiences

When: Saturday, Aug 8, 12:45 - 13:45 PDT

Where: LVCCW Level 1 Hall 2 604 (Appsec Village) Arsenal - [Map](#)

Description:

OWASP FinBot is an intentionally vulnerable agentic AI application designed to teach real-world security risks in AI agents beyond prompt injection alone. This Arsenal session demonstrates how an AI assistant connected to business tools can be manipulated through indirect prompts, unsafe tool use, broken authorization, and weak runtime controls. Attendees will see and experience first-hand how attacker-controlled inputs can influence agent behavior, trigger unsafe actions, and expose sensitive data.

Speakers: Helen Oakley, saikishu

SpeakerBio: Helen Oakley

Helen Oakley, CISSP, GPCS, GSTRT, works at the intersection of AI, cybersecurity, and software supply chains—where the rules are still being written. At SAP, she leads a global team of architects, security experts, and scientists, securing development and pipelines at scale. Helen is part of the core leadership team of the OWASP GenAI Security Project and co-leads initiatives on AIBOM and Agentic Security, contributes into industry papers like Agentic AI Threats & Mitigations Guide, OWASP Top 10 for Agentic Apps, and more. Helen has co-led AIBOM efforts with CISA, and is the original creator of the OWASP FinBot CTF and the first open-source OWASP AIBOM Generator for Hugging Face models. Named one of the Top 20 Canadian Women in Cybersecurity, she co-founded LeadingCyberLadies.com to support the next wave of builders, breakers, and leaders.

SpeakerBio: saikishu

Venkata Sai Kishore Modalavalasa is Chief Architect & Engineering Leader at Straiker, building AI security products for AI-native apps at scale. With 15+ years in cybersecurity and distributed systems, he scaled Cyberfend to acquisition by Akamai, where he led bot detection and web security engineering. He's an OWASP author contributing to AI Exchange, AIBOM, Top 10 for Agentic Applications, OWASP GenAI Security Project, creator and co-lead of OWASP FinBot CTF, and holds multiple security patents.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: OWASP ISTG in Practice: A CTF-Style IoT Hacking & Defending Lab

Tags: OWASP Foundation | Creator Workshop

When: Friday, Aug 7, 12:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 4 1415 (OWASP Foundation) - [Map](#)

Description:

Step into the world of ethical hacking and uncover the unseen vulnerabilities hiding inside everyday connected devices. This immersive, beginner-friendly lab teaches IoT security the way professionals actually practice it — using the OWASP IoT Security Testing Guide (ISTG) as your map — wrapped in an approachable Capture-the-Flag format, and led by the team that authors and field-tests the methodology.

No experience necessary. Just bring your curiosity. Whether you're a student, a tech enthusiast, or someone eyeing a cybersecurity career, this session makes real device hacking accessible, hands-on, and genuinely fun.

Working against a custom-built networking device, you'll follow the ISTG methodology from the outside in. You'll start at the hardware: reading and interpreting physical signals to locate and identify an exposed UART interface (ISTG-PHY, ISTG-INT) — the kind of serial debug port that, in real-world assessments, hands attackers an unauthenticated root shell within minutes of opening the enclosure. Unlocking that interface opens a cyber range where you'll pivot through firmware secrets (ISTG-FW), then practice attacks at the network and application layers — each flag mapped back to an ISTG test-case category, so you leave understanding not just how you got in, but how the risk is classified and defended.

By the end, you'll have a repeatable, standards-based mental model for testing any connected device — and a firsthand look at the most overlooked risks living inside the networks we all rely on.

Speakers: Piero "p33_p33_" Picasso, Aaron Guzman

SpeakerBio: Piero "p33_p33_" Picasso, Senior Security Leader at Cisco

Piero Picasso (p33_p33_) is a Senior Security Leader for Device Penetration Testing at Cisco, where he leads security testing for network infrastructure and IoT devices. Based in the Fort Lauderdale area, he brings over 20 years of experience in offensive security, penetration testing, and product security engineering. Over five-plus years at Cisco — including as Offensive Security Leader at Cisco Meraki — he built and scaled security testing programs for cloud-managed networking products. Earlier, he assessed Fortune 500 clients as a penetration tester at Secureworks and led ethical hacking within Citi's regulated financial environment. He continues to advance Cisco's device security posture through hands-on testing methodologies and cross-functional security research.

SpeakerBio: Aaron Guzman, Project Leader at OWASP

Aaron Guzman is CISO of Cisco Network Product Engineering, the organization responsible for securing Cisco's enterprise and industrial networking portfolio — from wireless access points, routers, and switches to IoT cameras and sensors — much of the infrastructure that moves the world's data. He is the author of the IoT Penetration Testing Cookbook and a technical reviewer for Practical IoT Hacking and Bug Bounty Bootcamp. As OWASP's IoT Project Leader, he leads the IoT Security Testing Guide (ISTG) — the very methodology at the heart of this lab. He started as a hacker, driven by a curiosity to take things apart and make them do what they were never designed to — a curiosity that now scales across hardware, firmware, supply chains, and software at enterprise scale.



Queercon Community - Saturday - 14:00-14:59 PDT

Title: Own the con

Tags: Queercon Community | Creator Talk/Panel

When: Saturday, Aug 8, 14:00 - 14:59 PDT

Where: LVCCW Level 3 W325 (QueerCon Lounge) - [Map](#)

Description:

A talk about Queercon and you

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

The Diana Initiative - Friday - 11:10-11:20 PDT

Title: Packet Hacking Village Tour

Tags: The Diana Initiative | Creator Tour

When: Friday, Aug 7, 11:10 - 11:20 PDT

Where: LVCCW Level 1 South Lobby / Atrium - [Map](#)

Description:

Interested in visiting Packet Hacking Village but afraid to go by yourself? The Diana Initiative is hosting tours! Follow a volunteer to Packet Hacking Village and be introduced to the community and activities inside!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Social Gatherings/Events - Saturday - 21:00-00:59 PDT

Title: Party Line (Call Center Village Party)

Tags: Party | Call Center Village

When: Saturday, Aug 8, 21:00 - 00:59 PDT

Where: LVCCW Level 2 W218 (Call Center Village) - [Map](#)

Description:

You've been placed on hold — but for once, you don't mind the music.

Party Line is Call Center Village's telephony-themed party open to all attendees at DEF CON 34.

A full-size telephone booth, retro telephones, dial-pad light shows, and lo-fi hold music grooves mixed with telephony-flavored party tracks.

If you've ever listened to Opus No. 1 on repeat, then this is your extension. No IVR to navigate Just pick up and dial in.

Don't let the phones go unanswered. Join us at Party Line.

Between calls, swing by our unofficial DEF CON TCG trading table — donate your extras, hunt down the ones you're missing, or make a deal for your favorites.

Make sure to bring your Call Center Village flight-tags (100 Trying or 200 OK) earned from the Escalation Desk CTF to claim free drinks!

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Past the Bouncer: The Limits of CSP, Eleven Years In

Tags: Intermediate | AppSec Village | Creator Talk/Panel

When: Saturday, Aug 8, 11:50 - 12:20 PDT

Where: LVCCW Level 1 Hall 2 604 (Appsec Village) Main Stage - [Map](#)

Description:

CSP turned eleven this year. It is the standard the web ultimately adopted to decide which scripts a page is allowed to load and execute, and it now sits at the center of how we think about XSS mitigation, third-party script risk, and client-side supply-chain compromise.

The problem is that CSP was designed as a fetch-time control. It evaluates origins, nonces, hashes, and directives when resources are requested, yet it is often expected to provide guarantees about what trusted code does after execution begins. The bypass literature tells a different story.

This talk examines five representative CSP bypass classes, and uses them to expose the gap between controlling what may be loaded and governing behaviour at runtime. It also raises broader questions of script governance, supply-chain security, and the distinction between fetch-time and runtime security controls.

I conclude by introducing an open learning platform that contains a comprehensive catalogue of CSP bypass techniques.

SpeakerBio: Pedro Fortuna

Pedro Fortuna is a security researcher, entrepreneur, and CTO of Jscrambler. For more than 15 years, his work has focused on web security, client-side security, reverse engineering, malware analysis, and software supply chain threats. He is the author of multiple security patents, a contributor to OWASP, and a member of the PCI Security Standards Council Board of Advisors.

Pedro regularly presents security research at international conferences and spends much of his time investigating how modern web applications fail in practice, from browser-side attacks and web skimming campaigns to the security implications of emerging technologies.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Patch Gap to Mobile Renderer RCE: Pwning Samsung Internet's V8 on the Galaxy S25

Tags: DEF CON Official Talk | Demo | Exploit

When: Friday, Aug 7, 12:30 - 13:30 PDT

Where: LVCCW Level 1 Hall 3 904 (Main Track 4) - [Map](#)

Description:

What happens when a flagship phone like the Samsung Galaxy S25 ships with an outdated Javascript engine in its default browser?

For the past 6 months, Samsung Internet shipped with an out-of-date V8 build that had already-fixed, publicly known vulnerabilities. One such bug is CVE-2025-10891, a flaw in Ignition bytecode generation for Javascript exception handling. In this talk, we show how we transform this vulnerability into reliable renderer code execution through instruction smuggling and internal native V8 runtime calls. We then showcase how we exploit weaker isolation mechanisms on mobile Chromium engines to upgrade the renderer RCE's capability into a universal XSS primitive.

<https://osec.io/blog/2026-04-01-patch-gap-to-mobile-renderer-rce/> <https://issuetracker.google.com/issues/443875388>

Speakers: Hrvoje Mišetić, Jamie Hill-Daniel, William Liu

SpeakerBio: Hrvoje Mišetić, OtterSec

Hrvoje Mišetić is a Web3 auditor and security researcher at OtterSec with prior research projects including Linux kernel LPE, QEMU hypervisor escape, and browser exploitation. He is a member of the Crusaders of Rust CTF team, and DiceGang, with whom he has qualified for Defcon CTF Finals multiple times. He presented Minecraft RCE research at OffensiveCon '26.

SpeakerBio: Jamie Hill-Daniel, OtterSec

Jamie Hill-Daniel is a security auditor currently working at OtterSec, with an interest in browser and kernel research. He is a member of the Crusaders of Rust and DiceGang CTF teams, having qualified for multiple Defcon CTF Finals with the latter.

SpeakerBio: William Liu

William Liu is a security engineer at Trail of Bits with experience in low-level systems and computer architecture. He is a member of the Crusaders of Rust and DiceGang CTF teams, having qualified for multiple Defcon CTF Finals with the latter. He has previously worked as a systems software engineer at NVIDIA. He documents some of his research on his personal site, willsroot.io.

William is a Class of 2025 graduate of the Massachusetts Institute of Technology, where he worked on the EntryBleed KASLR bypass and kernel fuzzing under Professor Mengjia Yan. He has presented micro-architectural security research at HASP '23 and NEHWS '24, as well as Linux 0-day research at Hexacon '25.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Patch Me If You Can: Hands-On Network Threat Defense

Tags: Cloud Village | Creator Event/Activity | Investigation

When: Saturday, Aug 8, 11:00 - 12:59 PDT

Where: LVCCW Level 3 W311 (Cloud Village Labs) A - [Map](#)

Description:

Join this hands-on workshop to explore an integrated set of network security capabilities designed for real-time threat detection, prevention, and proactive risk management. You'll see how inline traffic inspection can block threats with virtual patching, helping reduce exposure before vendor patches are available.

The session will also cover how deep network visibility supports detection of command-and-control activity, lateral movement, and advanced malware using behavioral analysis and custom sandboxing. You'll learn how continuous asset monitoring can uncover misconfigurations, exposure, and other risk factors across the environment, then use that insight to prioritize response and reduce overall risk.

SpeakerBio: Don Bogert

With more than 25 years of experience in cybersecurity, Don brings a comprehensive approach to organizational defense. Grounded in a strong network security foundation, his expertise spans physical security, compliance auditing, and the deployment of cloud, workload, and endpoint solutions. Throughout his career, Don has secured commercial, federal, and public sector organizations globally; and understands the challenges of a secure air-gapped environment. Currently, he focuses on delivering tailored security solutions to public sector customers in the Northeastern United States.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Pattern, Graph, Prompt: What Happens When You Layer Three Analysis Paradigms on the Same Codebase

Tags: Intermediate | AppSec Village | Creator Talk/Panel

When: Saturday, Aug 8, 14:50 - 15:20 PDT

Where: LVCCW Level 1 Hall 2 604 (Appsec Village) Main Stage - [Map](#)

Description:

We ran three fundamentally different security analysis approaches against the same production monorepo at a large tech company: a pattern-based static analysis tool, a code property graph analyzer, and LLM-powered code review. Together they surfaced over 100 confirmed vulnerabilities.

Each approach has real strengths and real limitations. Pattern-based static analysis is fast and deterministic but struggles with complex taint propagation and cannot reason about logic. Graph-based analysis can trace dataflow across the entire codebase but has no concept of developer intent. LLM-powered review can reason about whether a security mechanism actually does what it claims, but it is non-deterministic, expensive, and cannot guarantee exhaustive coverage the way a static tool can. We present a practical methodology for layering these approaches, share the detection overlap data from our analysis, and provide a framework for deciding which paradigm to apply where.

SpeakerBio: Mudita Khurana

Mudita Khurana is a Tech Lead at Airbnb, where she builds scalable security tooling and automation across the software development lifecycle. Previously at Meta, she drove key initiatives in product security, including bug bounty strategy, privacy-focused reviews, and automated vulnerability detection through static and hybrid analysis. Her work focuses on advancing security automation through robust workflows, agentic systems, and scalable system design. Mudita also serves on program committees for several top-tier security conferences and regularly contributes to the community through research, talks, and industry collaborations.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Payment Village - Saturday - 10:30-10:45 PDT

Title: Payment Village Intro - What's Happening at the Village

Tags: Payment Village | Creator Workshop

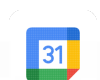
When: Saturday, Aug 8, 10:30 - 10:45 PDT

Where: LVCCW Level 2 W204-205 (Payment Village) - [Map](#)

Description:

Join us to discover some of the highlights of the Payment Village at DEF CON

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Payment Village - Friday - 10:30-10:45 PDT

Title: Payment Village Intro - What's Happening at the Village

Tags: Payment Village | Creator Workshop

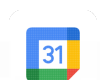
When: Friday, Aug 7, 10:30 - 10:45 PDT

Where: LVCCW Level 2 W204-205 (Payment Village) - [Map](#)

Description:

Join us to discover some of the highlights of the Payment Village at DEF CON

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

The Diana Initiative - Saturday - 10:40-10:50 PDT

Title: Payment Village Tour

Tags: The Diana Initiative | Creator Tour

When: Saturday, Aug 8, 10:40 - 10:50 PDT

Where: LVCCW Level 1 South Lobby / Atrium - [Map](#)

Description:

Interested in visiting Payment Village but afraid to go by yourself? The Diana Initiative is hosting tours! Follow a volunteer to Payment Village and be introduced to the community and activities inside!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Peekaboo: Breaking the Black Box of Threat and Malware Emulation

Tags: DEF CON Demo Labs | Intermediate | Defense/Blue Team | Malware | Offense/Red Team | Purple Team | Threat Intel/Hunting | DEF CON Demo Labs

When: Friday, Aug 7, 10:00 - 10:45 PDT

Where: LVCCW Level 1 Hall 3 1002 (Demo Labs Track 2) - [Map](#)

Description:

Standard security testing often forces a choice: use "script-kiddie" tools that get caught instantly, or use high-end frameworks that are too complex for rapid detection testing. Peekaboo bridges this gap. In this Demo Lab, we present Peekaboo - a modular, open-source framework designed for safe threat emulation. Unlike traditional malware, Peekaboo focuses on generating high-fidelity telemetry through legitimate cloud API abuse (GitHub, Bitbucket, Slack, Discord, Azure, VirusTotal, XBOX, AngelCam, etc) and evasive execution techniques (Direct Syscalls, Callback-based execution).

We will demonstrate how to:

- Generate polymorphic agents that bypass static analysis using rare cryptographic algorithms like Speck and Skipjack.
- Generate agents that leverage signal processing like Fast Fourier Transformation and Feistel-network based cryptography for bypass EDR.
- Establish covert C2 channels within the metadata of trusted enterprise applications.
- Rapidly test EDR/SIEM rules against modern persistence and lateral movement techniques without risking system stability.

Peekaboo isn't just a tool; it's a "sandbox-friendly" adversary in a box, designed to help Blue Teams level up by understanding the nuances of the Offensive Dev Loop. Come see how we turn "hidden" threats into "visible" learning opportunities.

SpeakerBio: Zhassulan "cocomelonc" Zhussupov

cybersecurity enthusiast, author, speaker and mathematician. Author of popular books: MD MZ Malware Development Book (Github, 2022, 2024) MALWILD: Malware in the Wild Book (Github, 2023) Malware Development for Ethical Hackers Book: (Packt, 2024) AIYA Mobile Malware Development Book (Github, 2025) Malware Development for Ethical Hackers 2nd edition (Packt, 2026, in progress) Author and tech reviewer at Packt. Co founder of various cybersecurity research labs, author of many cybersecurity blogs, HVCK magazine Malpedia contributor Speaker at BlackHat, DEFCON, Security BSides, Arab Security Conference, Hack.lu, Standoff, Positive Hack Talks, etc conferences

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Peekaboo: Breaking the Black Box of Threat and Malware Emulation

Tags: DEF CON Demo Labs | Intermediate | Defense/Blue Team | Malware | Offense/Red Team | Purple Team | Threat Intel/Hunting | DEF CON Demo Labs

When: Saturday, Aug 8, 10:00 - 10:45 PDT

Where: LVCCW Level 1 Hall 3 1002 (Demo Labs Track 2) - [Map](#)

Description:

Standard security testing often forces a choice: use "script-kiddie" tools that get caught instantly, or use high-end frameworks that are too complex for rapid detection testing. Peekaboo bridges this gap. In this Demo Lab, we present Peekaboo - a modular, open-source framework designed for safe threat emulation. Unlike traditional malware, Peekaboo focuses on generating high-fidelity telemetry through legitimate cloud API abuse (GitHub, Bitbucket, Slack, Discord, Azure, VirusTotal, XBOX, AngelCam, etc) and evasive execution techniques (Direct Syscalls, Callback-based execution).

We will demonstrate how to:

- Generate polymorphic agents that bypass static analysis using rare cryptographic algorithms like Speck and Skipjack.
- Generate agents that leverage signal processing like Fast Fourier Transformation and Feistel-network based cryptography for bypass EDR.
- Establish covert C2 channels within the metadata of trusted enterprise applications.
- Rapidly test EDR/SIEM rules against modern persistence and lateral movement techniques without risking system stability.

Peekaboo isn't just a tool; it's a "sandbox-friendly" adversary in a box, designed to help Blue Teams level up by understanding the nuances of the Offensive Dev Loop. Come see how we turn "hidden" threats into "visible" learning opportunities.

SpeakerBio: Zhassulan "cocomelonc" Zhussupov

cybersecurity enthusiast, author, speaker and mathematician. Author of popular books: MD MZ Malware Development Book (Github, 2022, 2024) MALWILD: Malware in the Wild Book (Github, 2023) Malware Development for Ethical Hackers Book: (Packt, 2024) AIYA Mobile Malware Development Book (Github, 2025) Malware Development for Ethical Hackers 2nd edition (Packt, 2026, in progress) Author and tech reviewer at Packt. Co founder of various cybersecurity research labs, author of many cybersecurity blogs, HVCK magazine Malpedia contributor Speaker at BlackHat, DEFCON, Security BSides, Arab Security Conference, Hack.lu, Standoff, Positive Hack Talks, etc conferences

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Pentester vs AI: Race The Machine, In Real Life

Tags: AppSec Village | Creator Event/Activity || All Audiences

When: Saturday, Aug 8, 11:00 - 12:59 PDT

Where: LVCCW Level 1 Hall 2 604 (Appsec Village) POD 2 - [Map](#)

Description:

The machine already solved it. Could you? Pentester vs AI brings our race-the-machine CTF off the screen and onto the table. Draw a card, read the challenge, a leaky query, a forged token, a broken access check, and walk us through how you'd break it. No laptop, no flag to submit. Just talk through your approach: what's the flaw, what would you reach for, where's the path in. Then flip the card and see how the AI reasoned through the same target. Where you agreed, where you didn't. The clock is ticking for each challenge; come show us your line.

Speakers:Gwendal Mognier,Samantha Pearlstein

SpeakerBio: Gwendal Mognier

Gwendal Mognier is a Security Researcher at Escape. He's passionate about cybersecurity and always eager to learn new ways to break and secure systems. Gwendal is focused on discovering vulnerabilities and helping improve security across the board.

SpeakerBio: Samantha Pearlstein, Founding Solutions Engineer at Escape

Samantha is a solutions engineer with a strong background in security research, executive cyber resilience, and nation-state threats. As a former consultant at Accenture, she led cyber resilience initiatives for Fortune 100 executives, developed GenAI-powered security tools, and delivered workshops on emerging cyber challenges. Today, as a Sales Engineer at Escape, Samantha helps AppSec teams secure their APIs and SPAs, combining her passion for cybersecurity with hands-on problem-solving.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: PentestGPT: The Art of Hacking with Words

Tags: La Villa Community | Creator Workshop

When: Friday, Aug 7, 14:00 - 15:59 PDT

Where: LVCCW Level 1 Hall 4 1416 (La Villa Community) Workshops/Chillout - [Map](#)

Description:

PentestGPT: The Art of Hacking with Words regresa a DEF CON, esta vez como un workshop completamente práctico. Luego de presentar el año pasado cómo los LLMs comenzaban a transformar la seguridad ofensiva, esta nueva edición lleva la experiencia al siguiente nivel: no solo será escuchar de este proyecto, lo podrás crear y ejecutar en tu entorno favorito.

Durante 100 minutos, los participantes trabajarán directamente con PentestGPT y PentestGPT 2.0 para aprender cómo integrar IA en flujos reales de pentesting. A través de ejercicios guiados y escenarios ofensivos realistas, explorarán reconocimiento asistido por IA, generación de attack paths, análisis de hallazgos, prompt engineering ofensivo y validación técnica de resultados.

Más allá de usar una herramienta, el workshop propone un cambio de mentalidad: entender cómo pasar de ejecutar tareas manuales a orquestar inteligencia ofensiva.

SpeakerBio: Matias Armándola, Cybersecurity Lead, Proffesor and Speaker

I'm Mati Armándola, an Information Security leader with over 20 years of experience in technology and more than a decade dedicated exclusively to asset protection, regulatory compliance, and organizational culture.

I have led teams and projects in companies with regional reach and have participated as an international speaker at conferences such as Ekoparty, DevOpsDays, Nerdearla, and DEF CON, addressing topics such as offensive security, awareness, applied AI, and governance.

In addition to my work as a teacher at various institutions and educational platforms, training the next generation of professionals in security, cloud computing, and leadership.

My motto is LEAD – TEACH – PROTECT

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Pentesting made easy - Keeping sessions alive with session chains

Tags: AppSec Village | Creator Event/Activity || All Audiences

When: Friday, Aug 7, 10:15 - 11:15 PDT

Where: LVCCW Level 1 Hall 2 604 (Appsec Village) Arsenal - [Map](#)

Description:

Modern web applications require pentesters to manage multiple accounts, roles, and tenants while dealing with short-lived sessions, multi-step logins, and MFA. This complexity regularly breaks authenticated tooling and slows down assessments, forcing testers into repetitive manual re-authentication.

Our open-source tool, session-chains, addresses this challenge by automatically creating and maintaining authenticated sessions for any number of users. Testers define reusable authentication flows, while the tool keeps sessions valid in the background and exposes them to other tools.

It integrates with Burp Suite and CLI tools like sqlmap, enabling consistent authenticated testing even in complex environments. This allows security professionals to spend less time on authentication hurdles and more time identifying impactful vulnerabilities.

Speakers: Kai Glauber, Matthias Göhring

SpeakerBio: Kai Glauber

Kai Glauber is a senior security consultant and penetration tester at usd AG with experience in web application pentests, SSO assessments and Kubernetes security. With a background in software development, his early work in software testing led him to specialize in the security domain. He's passionate about workflow automation and making pentesting more efficient.

SpeakerBio: Matthias Göhring

Matthias Göhring is security consultant and penetration tester at usd AG, an information security company based in Germany with the mission #moresecurity. He is Head of usd HeroLab, the division of usd specialized in technical security assessments. In addition, he holds lectures at Technical University Darmstadt and University of Applied Sciences Darmstadt on ethical hacking and penetration testing. In previous scientific work, he focused on network and communication security as well as software security.

Previous publications: - Catching the Clones – Insights in Website Cloning Attacks, Risk Connect Conference, 2021 - Path MTU Discovery Considered Harmful, IEEE 38th International Conference on Distributed Computing Systems (ICDCS), 2018 - Tor Experimentation Tools, IEEE Security and Privacy Workshops, 2015 - On randomness testing in physical layer key agreement, IEEE 2nd World Forum on Internet of Things (WF-IoT), 2015

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Phasmid: Deniable Storage for Rubber-Hose Scenarios

Tags: DEF CON Demo Labs | Intermediate | Defense/Blue Team | Hardware/IoT | SecOps | DEF CON Demo Labs

When: Saturday, Aug 8, 12:00 - 12:45 PDT

Where: LVCCW Level 1 Hall 3 1001 (Demo Labs Track 1) - [Map](#)

Description:

Phasmid is a prototype deniable storage system built for a problem ordinary encryption handles poorly: what happens when the attacker stops attacking the math and starts coercing the human holding the key. It implements the Janus Eidolon System, or Janus System, a coercion-aware storage method that explores how visible disclosure and true protected state can diverge through deniable cryptographic structure, local-only operation, dual-profile storage, camera-based object-image matching, and owner-controlled destructive actions. Framed by the question of Agency, the project asks how a user can retain meaningful control over disclosure when physical pressure breaks normal cryptographic assumptions. This demo presents a practical low-power implementation on Raspberry Pi Zero 2 W for hostile situations where the attacker targets the person rather than the cipher.

SpeakerBio: Makoto "Mr.Rabbit" Sugita

Makoto Sugita is a security engineer and security toolmaker focused on practical systems for hostile environments, where cryptographic assumptions break down under real-world pressure. His work sits at the intersection of cryptography, hardware, and adversarial human behavior. He has presented tools and research at venues including Black Hat Arsenal and BSides, and is interested in deniable systems, tactical hardware, and building prototypes that expose uncomfortable but real security problems.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Phasmid: Deniable Storage for Rubber-Hose Scenarios

Tags: DEF CON Demo Labs | Intermediate | Defense/Blue Team | Hardware/IoT | SecOps | DEF CON Demo Labs

When: Friday, Aug 7, 16:00 - 16:45 PDT

Where: LVCCW Level 1 Hall 3 1001 (Demo Labs Track 1) - [Map](#)

Description:

Phasmid is a prototype deniable storage system built for a problem ordinary encryption handles poorly: what happens when the attacker stops attacking the math and starts coercing the human holding the key. It implements the Janus Eidolon System, or Janus System, a coercion-aware storage method that explores how visible disclosure and true protected state can diverge through deniable cryptographic structure, local-only operation, dual-profile storage, camera-based object-image matching, and owner-controlled destructive actions. Framed by the question of Agency, the project asks how a user can retain meaningful control over disclosure when physical pressure breaks normal cryptographic assumptions. This demo presents a practical low-power implementation on Raspberry Pi Zero 2 W for hostile situations where the attacker targets the person rather than the cipher.

SpeakerBio: Makoto "Mr.Rabbit" Sugita

Makoto Sugita is a security engineer and security toolmaker focused on practical systems for hostile environments, where cryptographic assumptions break down under real-world pressure. His work sits at the intersection of cryptography, hardware, and adversarial human behavior. He has presented tools and research at venues including Black Hat Arsenal and BSides, and is interested in deniable systems, tactical hardware, and building prototypes that expose uncomfortable but real security problems.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Contests - Saturday - 10:00-17:59 PDT

Title: PhreakMe

Tags: PhreakMe | Contest

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 210 (PhreakMe) - [Map](#)

Description:

Ever wondered what hacking looked like in the golden age of phone phreaking? What about today? What can we learn about the old techniques that still plague our current infrastructure? The PhreakMe Capture the Flag brings you the classic art of telecom exploitation.

The Hacked Existence team is once again hosting a telecom based CTF. The CTF runs on real live VoIP lines routed through a modified asterisk PBX allowing participants to dial in to the CTF from anywhere in the world. This number is live 24/7 throughout DEFCON, allowing you to hunt the PBX for flags any time, day or night. Don't have a phone? Come test your skills at one of our 5 payphones! Also there's a BBS, hope you brought your modem!

All the flags are based around historically accurate tactics, techniques, and procedures to manipulate emulated old school switching systems.

The purpose of our contest is to bring awareness around the still existing weaknesses in our telecom infrastructure and Interactive Voice Response Systems. Ideally visitors to our contest area will participate in the CTF allowing them to get a better understanding of telecom hacking in the year 2026 as well as a respect for the art of phreaking from yesteryear.

Come test your skills, challenge your knowledge, and dive deep into the world of phreaks.

Hints: Read 'The Cyberthief and the Samurai' and 'Masters of Deception: The Gang That Ruled Cyberspace' for a leg up.

Participant Prerequisites

A phone, or access to a phone that can dial an american based phone number. The BBS will be both accessible from a modem and also ssh. Ideally people will read books like 'The Cyberthief and the Samurai' and 'Masters of Deception: The Gang That Ruled Cyberspace' and the Cult of the Dead Cow book.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: PhreakMe

Tags: PhreakMe | Contest

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 210 (PhreakMe) - [Map](#)

Description:

Ever wondered what hacking looked like in the golden age of phone phreaking? What about today? What can we learn about the old techniques that still plague our current infrastructure? The PhreakMe Capture the Flag brings you the classic art of telecom exploitation.

The Hacked Existence team is once again hosting a telecom based CTF. The CTF runs on real live VoIP lines routed through a modified asterisk PBX allowing participants to dial in to the CTF from anywhere in the world. This number is live 24/7 throughout DEFCON, allowing you to hunt the PBX for flags any time, day or night. Don't have a phone? Come test your skills at one of our 5 payphones! Also there's a BBS, hope you brought your modem!

All the flags are based around historically accurate tactics, techniques, and procedures to manipulate emulated old school switching systems.

The purpose of our contest is to bring awareness around the still existing weaknesses in our telecom infrastructure and Interactive Voice Response Systems. Ideally visitors to our contest area will participate in the CTF allowing them to get a better understanding of telecom hacking in the year 2026 as well as a respect for the art of phreaking from yesteryear.

Come test your skills, challenge your knowledge, and dive deep into the world of phreaks.

Hints: Read 'The Cyberthief and the Samurai' and 'Masters of Deception: The Gang That Ruled Cyberspace' for a leg up.

Participant Prerequisites

A phone, or access to a phone that can dial an american based phone number. The BBS will be both accessible from a modem and also ssh. Ideally people will read books like 'The Cyberthief and the Samurai' and 'Masters of Deception: The Gang That Ruled Cyberspace' and the Cult of the Dead Cow book.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: PhreakMe

Tags: PhreakMe | Contest

When: Sunday, Aug 9, 10:00 - 11:59 PDT

Where: LVCCW Level 1 Hall 1 210 (PhreakMe) - [Map](#)

Description:

Ever wondered what hacking looked like in the golden age of phone phreaking? What about today? What can we learn about the old techniques that still plague our current infrastructure? The PhreakMe Capture the Flag brings you the classic art of telecom exploitation.

The Hacked Existence team is once again hosting a telecom based CTF. The CTF runs on real live VoIP lines routed through a modified asterisk PBX allowing participants to dial in to the CTF from anywhere in the world. This number is live 24/7 throughout DEFCON, allowing you to hunt the PBX for flags any time, day or night. Don't have a phone? Come test your skills at one of our 5 payphones! Also there's a BBS, hope you brought your modem!

All the flags are based around historically accurate tactics, techniques, and procedures to manipulate emulated old school switching systems.

The purpose of our contest is to bring awareness around the still existing weaknesses in our telecom infrastructure and Interactive Voice Response Systems. Ideally visitors to our contest area will participate in the CTF allowing them to get a better understanding of telecom hacking in the year 2026 as well as a respect for the art of phreaking from yesteryear.

Come test your skills, challenge your knowledge, and dive deep into the world of phreaks.

Hints: Read 'The Cyberthief and the Samurai' and 'Masters of Deception: The Gang That Ruled Cyberspace' for a leg up.

Participant Prerequisites

A phone, or access to a phone that can dial an american based phone number. The BBS will be both accessible from a modem and also ssh. Ideally people will read books like 'The Cyberthief and the Samurai' and 'Masters of Deception: The Gang That Ruled Cyberspace' and the Cult of the Dead Cow book.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Physical Security Village - Sunday - 11:00-11:59 PDT

Title: Physical Security is not sexy which is bad for organizations and good for red teams.

Tags: Physical Security Village | Creator Talk/Panel

When: Sunday, Aug 9, 11:00 - 11:59 PDT

Where: LVCCW Level 1 Hall 3 1104 (Creator Stage 4) - [Map](#)

Description:

With digital security tools continually becoming stronger, organizations often overlook their physical security as part of their operational security. Often, many organizations rely on their security integrators to secure the building. Those integrators business models are often not incentivized to properly secure the buildings. This leaves cameras, readers and keycards open for attackers and pen testers to exploit to gain access.

In this talk we'll discuss the shortcomings of access control door systems, how attackers and pen testers can use official tools from the manufactures to identify and exploit the readers and doors along with using tools like a Flipper, RFID USB readers and postcards.

SpeakerBio: Roger Egan

Roger is a washed up racecar driver with a more successful Information Systems career. This includes 10+ years experience in programming, installing, servicing and training on physical security software and equipment. Roger has shown organizations and law enforcement the strengths and weaknesses of physical security and how they can be exploited.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

The Diana Initiative - Friday - 10:50-10:59 PDT

Title: Physical Securty Village Tour

Tags: The Diana Initiative | Creator Tour

When: Friday, Aug 7, 10:50 - 10:59 PDT

Where: LVCCW Level 1 South Lobby / Atrium - [Map](#)

Description:

Interested in visiting Physical Securty Village but afraid to go by yourself? The Diana Initiative is hosting tours! Follow a volunteer to Physical Securty Village and be introduced to the community and activities inside!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Pickled and Exposed: RCE in AI Serving Frameworks

Tags: Intro/Beginner | AppSec Village | Creator Talk/Panel

When: Friday, Aug 7, 11:10 - 11:40 PDT

Where: LVCCW Level 1 Hall 2 604 (Appsec Village) Main Stage - [Map](#)

Description:

Your LLM serving stack is probably listening to the entire internet right now, and it will run whatever code that internet sends it. It will not ask who you are. Everyone is busy chasing prompt injection and jailbreaks. Meanwhile, the boring bugs are wide open. SGLang serves large language models for thousands of deployments, with 25k+ GitHub stars. I read the source and found two unauthenticated RCEs. There was nothing clever about it: a network-exposed broker hands attacker data straight to `pickle.loads()`. Send a payload, get a shell. I will walk the vulnerable code and pop a shell live on stage. You will leave knowing exactly what to grep for in your own AI stack, before someone else greps it for you. Two CVEs. One grep. Zero sophistication required.

SpeakerBio: Iggy

Igor Stepansky is a Security Researcher at OX Security, where he works on agentic AI for offensive security and automated penetration testing. Previously, he was part of Orca Security's Research Pod. His research spans unauthenticated remote code execution in AI/LLM serving frameworks, a use-after-free race condition in the Linux kernel's ksmbd SMB3 serve, and supply chain and CI/CD security across modern developer ecosystems. His work focuses on finding and exploiting high-impact vulnerabilities in widely deployed infrastructure, and he is a regular contributor of CVEs in open-source software.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Pickpocketing for Red Teamers: A Hands-On Experience

Tags: Social Engineering Community Village | Creator Event/Activity

When: Friday, Aug 7, 10:00 - 11:30 PDT

Where: LVCCW Level 3 W320 (Social Engineering Community Village Labs) - [Map](#)

Description:

Seven years ago, pradameinhof ran the world's first public pickpocketing competition with about 200 people at a social engineering conference. The inspiration? His dad got pickpocketed right next to him on the Paris Metro. What started as frustration turned into obsession' not just with preventing it, but with understanding how easy it is to pull off. It was hard enough finding good resources. The real problem? Testing your skills in realistic scenarios can land you in jail.

In this two-hour Social Engineering Community session, pradameinhof will teach what he learned: the core techniques of attention manipulation' directing and surfing attention, relative touch, entering personal space, giving shade, fanning, and working in teams. You'll learn to lift wallets, watches, phones, badges, and keys, and apply these skills to red-teaming.

Here's how it works: You'll pair up and take turns' one practitioner, one target. No prior experience necessary.

What to bring: A jacket and pants with pockets that aren't too tight. Wear a watch if you have one. Because you will need to steal from other people and be pickpocketed, expect to touch and be touched by others in order to participate' all appropriately and with clear consent.

Join us in this group exercise to understand the human blind spots that make physical social engineering so effective. Walk away with skills for your next red-team engagement' and better awareness so you don't become a target.

(Disclaimer: This exercise is for educational purposes only. If you pickpocket people without their consent, expect to get into trouble.)

SpeakerBio: pradameinhof

pradameinhof has worked in cyber security startups for over two decades. Most of his skills he acquired by pestering his friends and colleagues over coffee. He has a passion for OSINT and Social Engineering.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Contests - Friday - 10:00-17:59 PDT

Title: Pinball High Score Contest

Tags: Pinball High Score Contest | Contest

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 304 (Pinball High Score Contest) - [Map](#)

Description:

The Pinball High Score contest at DEF CON 34 will run Friday and Saturday: 10:00-18:00, Sunday 10:00-13:00 with games available for daily High Score contests, daily challenges and open qualifying for a main tournament. The daily contests will allow any attendee to play pinball games and attempt to record a qualifying high score on each of the unique games. At 17:00 on Saturday main tournament qualifying will end, tiebreakers will be played (if needed) and the top 8 players with the highest combined scores across all eligible machines will qualify for the Sunday finals event where they could become the next DEF CON Pinball Champion!

Achieving a high score may sound simple but pinball rulesets are very complex and the skill to complete a “Wizard Mode” or achieve a high score requires research, practice, knowledge and execution. Out of the box thinking, analytical skills and pattern recognition are traits that pinball players must exhibit to be successful and some games have rule sets that can be studied and exploited to achieve a high score. Hackers are at an advantage here and while this is just a pinball contest, we expect that the community is ready for this challenge!

Last year the contest measured how you moved the machine. This year, we're reading what happens inside it. Custom sensors feed SHELL, our Sub-surface Hidden Entertainment Layer Logic. When you unlock the right patterns, a hidden world appears on screens beneath the glass. Face off in secret mini-games, answer hacker trivia under pressure, and battle other players in competitive challenges where you can steal control mid-game. It's pinball within pinball, a clandestine layer of gameplay that only reveals itself to those who can crack the SHELL.

Participant Prerequisites

Nothing special is required. Any person can step up and enjoy a pinball game or they can spend 30+ hours solving our challenges if they want to play the deeper game.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Contests - Saturday - 10:00-17:59 PDT

Title: Pinball High Score Contest

Tags: Pinball High Score Contest | Contest

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 304 (Pinball High Score Contest) - [Map](#)

Description:

The Pinball High Score contest at DEF CON 34 will run Friday and Saturday: 10:00-18:00, Sunday 10:00-13:00 with games available for daily High Score contests, daily challenges and open qualifying for a main tournament. The daily contests will allow any attendee to play pinball games and attempt to record a qualifying high score on each of the unique games. At 17:00 on Saturday main tournament qualifying will end, tiebreakers will be played (if needed) and the top 8 players with the highest combined scores across all eligible machines will qualify for the Sunday finals event where they could become the next DEF CON Pinball Champion!

Achieving a high score may sound simple but pinball rulesets are very complex and the skill to complete a “Wizard Mode” or achieve a high score requires research, practice, knowledge and execution. Out of the box thinking, analytical skills and pattern recognition are traits that pinball players must exhibit to be successful and some games have rule sets that can be studied and exploited to achieve a high score. Hackers are at an advantage here and while this is just a pinball contest, we expect that the community is ready for this challenge!

Last year the contest measured how you moved the machine. This year, we're reading what happens inside it. Custom sensors feed SHELL, our Sub-surface Hidden Entertainment Layer Logic. When you unlock the right patterns, a hidden world appears on screens beneath the glass. Face off in secret mini-games, answer hacker trivia under pressure, and battle other players in competitive challenges where you can steal control mid-game. It's pinball within pinball, a clandestine layer of gameplay that only reveals itself to those who can crack the SHELL.

Participant Prerequisites

Nothing special is required. Any person can step up and enjoy a pinball game or they can spend 30+ hours solving our challenges if they want to play the deeper game.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Contests - Sunday - 10:00-11:59 PDT

Title: Pinball High Score Contest

Tags: Pinball High Score Contest | Contest

When: Sunday, Aug 9, 10:00 - 11:59 PDT

Where: LVCCW Level 1 Hall 1 304 (Pinball High Score Contest) - [Map](#)

Description:

The Pinball High Score contest at DEF CON 34 will run Friday and Saturday: 10:00-18:00, Sunday 10:00-13:00 with games available for daily High Score contests, daily challenges and open qualifying for a main tournament. The daily contests will allow any attendee to play pinball games and attempt to record a qualifying high score on each of the unique games. At 17:00 on Saturday main tournament qualifying will end, tiebreakers will be played (if needed) and the top 8 players with the highest combined scores across all eligible machines will qualify for the Sunday finals event where they could become the next DEF CON Pinball Champion!

Achieving a high score may sound simple but pinball rulesets are very complex and the skill to complete a “Wizard Mode” or achieve a high score requires research, practice, knowledge and execution. Out of the box thinking, analytical skills and pattern recognition are traits that pinball players must exhibit to be successful and some games have rule sets that can be studied and exploited to achieve a high score. Hackers are at an advantage here and while this is just a pinball contest, we expect that the community is ready for this challenge!

Last year the contest measured how you moved the machine. This year, we're reading what happens inside it. Custom sensors feed SHELL, our Sub-surface Hidden Entertainment Layer Logic. When you unlock the right patterns, a hidden world appears on screens beneath the glass. Face off in secret mini-games, answer hacker trivia under pressure, and battle other players in competitive challenges where you can steal control mid-game. It's pinball within pinball, a clandestine layer of gameplay that only reveals itself to those who can crack the SHELL.

Participant Prerequisites

Nothing special is required. Any person can step up and enjoy a pinball game or they can spend 30+ hours solving our challenges if they want to play the deeper game.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Pinchy Gets Played: How We Red-Teamed AI Agents Before the Threats Did

Tags: Cloud Village | Creator Talk/Panel

When: Saturday, Aug 8, 12:20 - 12:59 PDT

Where: LVCCW Level 3 W313 (Cloud Village Talks) - [Map](#)

Description:

AI agents are showing up in cloud workflows with credentials, autonomy, and trust, but so are the threats targeting them. So, before attackers started probing them, Varonis Threat Labs did. We built a target agent named Pinchy on the OpenClaw platform and put it through a red-team gauntlet using well-known techniques. Pinchy handled sophisticated technical attacks with ease but folded immediately against simple social ones. The same drive to be useful turns these agents into an attack surface that requires entirely different defensive strategies. Join us for a deep dive on the new risks autonomous AI brings to the cloud. You'll leave with a clearer picture of where AI agents fail, why the threat model is unlike anything that came before it, and what architectural controls — not prompts, not policies — actually keep environments secure.

SpeakerBio: Doron Kapah

Doron is an experienced security researcher at Varonis Threat Labs. He primarily focuses on advanced threat detection capabilities, threat hunting, and AI and cloud security. Doron also has extensive experience in building innovative cybersecurity product solutions, CTFs and has authored multiple publications in both state-sponsored and cybercrime threat intelligence domains.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

IoT Village - Saturday - 10:30-11:45 PDT

Title: Playing with Hyper-local Pocket-Sized Servers

Tags: IoT Village | Creator Workshop

When: Saturday, Aug 8, 10:30 - 11:45 PDT

Where: LVCCW Level 1 Hall 1 215 (IoT Village) - [Map](#)

Description:

In this hands-on workshop, we'll turn an ESP8266 into a self-contained Wi-Fi pocket server that anyone nearby can connect to without the internet. Kit Cost: \$80. Class Cap: 30.

SpeakerBio: Brandon

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Maritime Hacking Village - Saturday - 12:00-12:30 PDT

Title: Please Place Your Electronic Devices in {Maritime} Mode: Exposing NTN's Maritime Attack Surface

Tags: Maritime Hacking Village | Creator Talk/Panel

When: Saturday, Aug 8, 12:00 - 12:30 PDT

Where: LVCCW Level 1 Hall 3 801 (Creator Stage 2) - [Map](#)

Description:

Many Mariners share a sigh of relief once the sight of shore disappears. Sail far enough from the mainland, and the distractions of the cellular world fade away. No bars. No signal. No problem. Cellular Non-Terrestrial Networks (NTN) have stolen that comfort. Ships have long relied on satellite communications for safe navigation and operations at sea. However, traditional threats to GPS, satellite broadband, and Iridium are being rapidly supplanted by Direct-to-Device (D2D) cellular connectivity via NTN. The same vulnerabilities that plagued its terrestrial ancestors are quietly following mariners out to sea. This talk provides a technical deep-dive into 4G and 5G NTN architecture, its current footprint in the maritime environment, and the vulnerabilities it inherits from its terrestrial ancestors. We close by charting a course forward, exploring open research questions and offering practical recommendations.

SpeakerBio: Jason Veara, Independent Researcher

Jason Veara is a Cybersecurity PhD student at Northeastern University, a Coast Guard Officer, and Permanent Military Faculty at the U.S. Coast Guard Academy in New London, CT. His research focuses on identity, localization and trust in wireless-dependent autonomous systems.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Plug And Pwn: Weaponizing Windows PnP Auto-Install

Tags: DEF CON Official Talk | Demo | Exploit

When: Friday, Aug 7, 13:30 - 14:30 PDT

Where: LVCCW Level 1 Hall 3 904 (Main Track 4) - [Map](#)

Description:

Every time a USB device is plugged into a Windows machine, the OS may silently download a package from Microsoft and execute vendor code as SYSTEM. No admin required. The package is signed, so nothing looks wrong.

We spent the better part of a year mapping this attack surface. We analyzed 7K packages approx, built tools to emulate arbitrary USB devices without hardware, and found that the same kernel code path fires when a USB device is redirected over RDP channels, meaning a non admin user can trigger SYSTEM level code execution on the target, with no physical access at all (under certain conditions).

- How Windows PnP search actually works, the real kernel flow, not the MSDN summary.
- How to make Windows believe any USB device is connected, using device emulation and composite device tricks that bypass inbox driver interception.
- Why RDP USB redirection (MS-RDPEUSB / URBDRC) triggers the exact same kernel PnP path as a physical plug-in, and what that means for remote exploitation.
- A WHQL-signed software that contains a hidden debug backdoor allowing execution as SYSTEM, chainable with other vulnerabilities for full user to SYSTEM escalation from a standard account.
- A forced installation leading to the creation of a named pipe that lets any authenticated network user rewrite config on any machine.

Speakers: Alejandro "0xedh" Hernando, Borja "borjnz" Martinez

SpeakerBio: Alejandro "0xedh" Hernando, Accenture Spain

Alejandro Hernando is a red team operator and security researcher at Accenture Security's Hacking team in Spain, with over a decade of hands-on experience in offensive cybersecurity. Throughout his career, he has assessed, exploited, and helped mitigate security vulnerabilities across commercial and proprietary systems, developing PoC exploits, offensive and defensive tooling, and conducting deep security research. His approach combines applied research with real world operational experience, driven by a focus on continuous learning and on sharpening both attack and defense strategies.

SpeakerBio: Borja "borjnz" Martinez, Accenture Spain

Borja Martínez is a red team operator and security researcher at Accenture Security Hacking team in Spain, where he focuses on offensive security, advanced adversary simulation and hardware exploitation. A self-taught hacker with a deeply hands-on approach, he specializes in red team operations, penetration testing and low level attack research including DMA attacks, BIOS/UEFI exploitation, and TPM security.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Red Team Village - Saturday - 10:00-11:59 PDT

Title: PMTC: One-Click RCE and Persistent Exfil in AI Coding Agents

Tags: Red Team Village | Misc

When: Saturday, Aug 8, 10:00 - 11:59 PDT

Where: LVCCW Level 1 Hall 1 309 (Red Team Village) Tactic Table 2 - [Map](#)

Description:

Red teamers operating in environments where developers run AI coding agents (Anthropic Claude Code, OpenAI Codex CLI) now have a high-impact, low-detection attack path. We call it PMTC (Persistent MCP Tool Capture). The live demo runs the full operational chain. A .lnk shortcut with hidden extension delivers the payload. One double-click launches the agent in attacker-controlled CWD. Parent-walk .mcp.json auto-exec fires. A zero-prompt OAuth flow captures credentials. A refresh token persists silently in the victim's home directory, re-authenticating every future session. OPSEC notes: cwd selection to defeat path-based logging, MCP server fingerprint reduction, OAuth state minimization. For blue teams: Sigma and Suricata rules included. You leave with the chain reproducer, .lnk template generator, and detection rules. Cross-vendor on Codex CLI. Disclosure in flight; CVEs released at the talk.

SpeakerBio: Ahmet Furkan Aydogan

Ahmet Furkan Aydogan is a Tenure-Track Assistant Professor in the Computer Science Department at the University of North Carolina Wilmington (UNCW). He earned his Ph.D. in Digital and Cyber Forensics Science from Sam Houston State University (SHSU) in 2024, with a focus on Cyber Security, Cryptology, Machine Learning, IoT, and Human-Computer Interaction. His research includes a Brain Frequency-Based Evolutionary Encryption Method for IoT Devices. Ahmet has received multiple awards and has published widely in the fields of cybersecurity and digital forensics.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Point of Failure: Autopsia de una Terminal de Pago

Tags: La Villa Community | Creator Talk/Panel

When: Friday, Aug 7, 14:00 - 14:59 PDT

Where: LVCCW Level 1 Hall 4 1416 (La Villa Community) Main Stage - [Map](#)

Description:

TPVs como PAX y Mercado Pago corren Android, usan HTTP en producción y tienen un modo kiosco que dura lo que tarda en abrirse un APK. Esta charla es el journey de alguien que compró terminales, las rompió, y documenta lo que encontró.

SpeakerBio: Erik Alcantara, I build the tools I can't afford.

Erik Alcantara aka. Glitchboi, es pentester y red teamer con 6 años en seguridad y enfoque en la intersección entre hardware y ofensiva. Desde México, construye herramientas open source que van desde proxies de interceptación HTTP hasta PCBs personalizadas para investigación de seguridad.

Ha presentado en BugCon y meetups locales de seguridad. Publica su research y proyectos en glitchboi.xyz y github.com/Glitchboi-sudo.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Poison the Well: RAG Attacks Against the Hacking Community's Own Archives

Tags: Data Duplication Village | Creator Talk/Panel

When: Saturday, Aug 8, 11:00 - 11:59 PDT

Where: LVCCW Level 2 W203 (Data Duplication Village) - [Map](#)

Description:

This presentation demonstrates how archive poisoning attacks compromise Retrieval-Augmented Generation (RAG) systems by embedding malicious instructions inside documents that influence model behavior during retrieval. Using a customized agentic testing workflow, attendees will see how a single poisoned document can manipulate outputs, exfiltrate sensitive information, bias threat intelligence results, and abuse trust relationships across a RAG-powered environment without modifying model weights.

SpeakerBio: Omer Farooq

Omer Farooq is a cybersecurity, cloud, and artificial intelligence leader with more than twenty-five years of experience spanning application security, cloud architecture, software engineering, DevSecOps, AI security, and technology innovation. As Founder and Principal Security Consultant at Auxin Security, Omer has advised more than 100 organizations worldwide, including Fortune 500 companies, government agencies, healthcare organizations, and nonprofits. His expertise includes GenAI and LLM security, offensive security assessments, threat modeling, cloud security, DevSecOps transformation, secure software development, and enterprise architecture. Omer is a frequent speaker at industry conferences and events including RSA Conference, BSides DC, AWS events, NAB Show, Microsoft Azure conferences, and numerous cybersecurity forums. His current research focuses on AI security, agentic systems, retrieval-augmented generation security, offensive AI testing, and emerging threats targeting enterprise AI deployments.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

The Diana Initiative - Saturday - 10:50-10:59 PDT

Title: Policy @ Defcon Tour

Tags: The Diana Initiative | Creator Tour

When: Saturday, Aug 8, 10:50 - 10:59 PDT

Where: LVCCW Level 1 South Lobby / Atrium - [Map](#)

Description:

Interested in visiting Policy @ Defcon but afraid to go by yourself? The Diana Initiative is hosting tours! Follow a volunteer to Policy @ Defcon and be introduced to the community and activities inside!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Social Gatherings/Events - Friday - 18:30-20:30 PDT

Title: Policy Mixer Happy Hour

Tags: Party | Policy @ DEF CON

When: Friday, Aug 7, 18:30 - 20:30 PDT

Where: LVCCW Level 2 W210-211 (Policy Village) - [Map](#)

Description:



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Polycon

Tags: Queercon Community | Creator Event/Activity

When: Saturday, Aug 8, 11:00 - 11:59 PDT

Where: LVCCW Level 3 W325 (QueerCon Lounge) - [Map](#)

Description:



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Poor Man's Mythos: Signal Siege: Agentic Exploit Chains Across the 5G Cloud-Native Stack

Tags: Telecom Village | Creator Talk/Panel

When: Friday, Aug 7, 12:30 - 13:15 PDT

Where: LVCCW Level 3 W321 (Telecom Village) - [Map](#)

Description:

1. 5G Attack Surface – New cloud-native risks and legacy trust issues.
2. Salt Typhoon – Lessons from real-world telecom breaches. NEF API Security – Exposed API attack vectors.
3. Signaling Exploitation – SS7/Diameter trust weaknesses in 5G. RAN-to-Core Pivoting – Lateral movement across telecom networks.
4. OSS/BSS Attacks – Exploiting IT–telecom integration.
5. Agentic AI – AI-driven telecom attack chain discovery.
6. Offensive AI – Lowering the barrier to advanced attacks.
7. Zero Trust for 5G – Securing telecom trust boundaries.
8. Control Plane Security – Prioritizing critical telecom risks.
9. Red Team Techniques – Practical telecom attack methodologies.

SpeakerBio: Omer Farooq

Omer Farooq is a cybersecurity, cloud, and artificial intelligence leader with more than twenty-five years of experience spanning application security, cloud architecture, software engineering, DevSecOps, AI security, and technology innovation. As Founder and Principal Security Consultant at Auxin Security, Omer has advised more than 100 organizations worldwide, including Fortune 500 companies, government agencies, healthcare organizations, and nonprofits. His expertise includes GenAI and LLM security, offensive security assessments, threat modeling, cloud security, DevSecOps transformation, secure software development, and enterprise architecture. Omer is a frequent speaker at industry conferences and events including RSA Conference, BSSides DC, AWS events, NAB Show, Microsoft Azure conferences, and numerous cybersecurity forums. His current research focuses on AI security, agentic systems, retrieval-augmented generation security, offensive AI testing, and emerging threats targeting enterprise AI deployments.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Post-Exploitation of the Desktop with JS-Tap

Tags: Red Team Village | Misc

When: Friday, Aug 7, 10:00 - 11:59 PDT

Where: LVCCW Level 1 Hall 1 309 (Red Team Village) Tactic Table 1 - [Map](#)

Description:

JS-Tap v3 moves beyond exploiting web applications to targeting the endpoint itself. JavaScript is used heavily on desktops and in this hands-on tactic you'll deploy three JS-Tap implant types against your own machine. Start by installing a malicious browser extension that harvests sessions from every site you visit and lets you inject payloads into specific apps on command. We'll then rebuild the browser extension implant with optional (and less stealthy) features that allow jumping from the browser to the operating system for filesystem/shell access.

Next we'll patch a local Electron app to get screenshots, keylogging, network interception, and filesystem/shell access. Then we'll instrument a Node.js tool with a single environment variable to intercept its network traffic, capture keystrokes, and get filesystem/shell access.

We'll use Docker containers to simulate an internal network with a web application your browser can't reach directly. You'll use the JS-Tap Conductor to clone captured sessions and pivot through an implant to access it, demonstrating the full attack chain from session theft to authenticated access on an internal network. Participants will run JS-Tap locally on their own laptops. Bring a machine with Chrome or Chromium, Firefox (for JS-Tap Conductor), a Node.js app (Gemini CLI, Claude Code, etc.), Docker, and at least one Electron app installed (VS Code or Signal Desktop work well as targets). Setup instructions will be shared in advance.

You'll leave with firsthand experience operating all three beacon types.

SpeakerBio: Drew Kirkpatrick

Drew has 25 years of experience designing and building complex systems, including application security, network policy management, machine learning, and transit and aerospace systems. These days he works to improve Information Security by applying penetration testing and computer science to assess the security posture of TrustedSec clients. Before joining TrustedSec, he was a Security Researcher at NopSec and Secure Decisions as well as a Senior Computer Scientist for the U.S. Navy.

Offensive Security Certified Professional (OSCP) GIAC Web Application Penetration Tester (GWAPT) GIAC Mobile Device Security Analyst (GMOB) M.S. Computer Science – Florida Institute of Technology M.S. Computer Information Systems – Florida Institute of Technology B.A. Psychology/Economics – St. Mary's College of Maryland



[Return to Index](#) - Add to Google - ics [Calendar](#) file

AI Village - Friday - 10:00-17:59 PDT

Title: Poster Presentations

Tags: AI Village | Creator Talk/Panel

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 2 603 (AI Village) - [Map](#)

Description:

AI Village is going old school academia with various presenters showcasing their research in poster format. Posters will be displayed on digital screens while presenters give conversational overviews of their research and invite casual discussions.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

AI Village - Saturday - 10:00-17:59 PDT

Title: Poster Presentations

Tags: AI Village | Creator Talk/Panel

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 2 603 (AI Village) - [Map](#)

Description:

AI Village is going old school academia with various presenters showcasing their research in poster format. Posters will be displayed on digital screens while presenters give conversational overviews of their research and invite casual discussions.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Practical AI Security Assessments Using OWASP AISVS

Tags: OWASP Foundation | Creator Workshop

When: Saturday, Aug 8, 16:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 4 1415 (OWASP Foundation) - [Map](#)

Description:

How do you actually verify that an AI system is secure? In this workshop, the AISVS project leads walk through practical assessment scenarios using the OWASP AI Security Verification Standard. We'll work through real requirements from chapters on prompt injection defense, agentic action security, RAG/vector database hardening, and output safety controls, showing what "verify that" looks like in practice against running systems. Participants will leave with a working understanding of how to scope an AI security assessment, select appropriate verification levels, and apply AISVS requirements to LLM-based applications, autonomous agents, and MCP-connected tool ecosystems. Bring a laptop if you want to follow along.

SpeakerBio: Jim Manico, Founder at Manicode Security

Jim Manico is the founder of Manicode Security, where he specializes in training software developers on secure coding and security engineering. He is actively involved in multiple ventures, serving as an investor/advisor for companies like 10Security, MergeBase, Nucleus Security, KSOC, and Inspectiv, among others. Jim is a recognized speaker, focusing on secure software practices, and holds a distinguished position as a member of the Java Champion community. He is also the esteemed author of "Iron-Clad Java: Building Secure Web Applications" published by Oracle Press.

Additionally, Jim generously volunteers for the OWASP foundation, co-leading key projects such as the OWASP Application Security Verification Standard and the OWASP Cheatsheet Series.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Noob Community - Friday - 10:00-13:50 PDT

Title: Practical Cybersecurity Skills in an AI-Augmented World: Protecting the AI Trifecta

Tags: Noob Community | Creator Workshop

When: Friday, Aug 7, 10:00 - 13:50 PDT

Where: LVCCW Level 1 Hall 4 1417 (Noob Community) - [Map](#)

Description:

The Ginger Hacker Initiative and CompTIA are teaming up for an interactive session focused on the three critical dimensions of AI cybersecurity: securing AI systems, securing with AI, and governing AI. Built directly around the new CompTIA SecAI+ course, this workshop completely bypasses the fluff to focus entirely on real-world application.

Speakers: James Stanger, Stephen Schneider

SpeakerBio: James Stanger

No BIO available

SpeakerBio: Stephen Schneider

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Practical Guidance for RF Researchers: Experiment First, Interfere Never

Tags: Radio Frequency Village | Creator Talk/Panel

When: Friday, Aug 7, 16:00 - 16:30 PDT

Where: LVCCW Level 1 Hall 3 1102 (Creator Stage 6) - [Map](#)

Description:

Practical Guidance for RF Researchers: Experiment First, Interfere Never. The world needs more experimentation. We want more high-quality experimentation that is reproducible, technically rigorous, and does not intentionally disrupt other spectrum users.

SpeakerBio: Andy Hendrickson, Independent Researcher, Washington DC

While at the Federal Communications Commission, I have had the opportunity to serve in two roles focused on advancing the nation's communications infrastructure and technology policy.

I currently serve as Chief of the Office of Engineering and Technology (OET), where I act as the FCC's principal technical advisor. In this role, I help shape national spectrum policy, oversee equipment authorization, experimental licensing, and guide the agency's technical direction to ensure regulatory frameworks keep pace with rapid innovation across the communications ecosystem.

Previously, I served as Chief Technology Officer for the FCC's Enforcement Bureau, providing strategic and technical leadership across cybersecurity, privacy, national security, robocall and robotext mitigation, network outage enforcement, and the protection of critical infrastructure such as 911 systems and GPS. I also advised the Office of the Field Director on technology and enforcement issues with national impact while coordinating closely with teams across the Commission.

In my downtime, I'm either deep in the world of audio recording and engineering or rocking out on various instruments.

Before joining the FCC, I spent more than two decades in the telecommunications industry, including leadership roles at Verizon supporting the rollout of 5G and the development of the Verizon Cloud Platform.

My background spans cloud computing, software-defined networking, virtualization, cybersecurity, and GIS, and I remain engaged with the broader technology community through organizations such as the Open Geospatial Consortium, Linux Foundation, Open Infrastructure Foundation, and Network Time Foundation.

I am honored to work alongside dedicated public servants and industry partners helping ensure the United States maintains secure, innovative, and resilient communications systems.

I hold dual degrees from Rutgers University, having studied at both the School of Environmental and Biological Sciences and the School of Communication and Information.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Practical Privacy Defenses for the Paranoid

Tags: OSINT For Good Community | Creator Talk/Panel

When: Sunday, Aug 9, 12:15 - 12:45 PDT

Where: LVCCW Level 1 Hall 4 1307 (OSINT4Good Community) Stage - [Map](#)

Description:

Public records, browser tracks, and digital footprints leave you exposed. Now, AI helps tie it all together even faster for anyone looking for information on a person. In this session, go deeper than data broker removals to improve your personal privacy habits and help mask your online identity. Entry-level and open to all skill levels and non-OSINT experts.

SpeakerBio: Tina "Hek8te" Shakour, Netwrix

Hek8te (Keeper of the Keys) brings two decades of cybersecurity experience to the front lines of blue team defense, protecting systems and people worldwide. A Senior Coach for Trace Labs and a veteran TechWomen volunteer, she is dedicated to global defense, OSINT, and community mentorship.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Red Team Village - Friday - 16:00-17:59 PDT

Title: Praetor: An OPSEC Exposure Advisor for Empire Operators

Tags: Red Team Village | Misc

When: Friday, Aug 7, 16:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 309 (Red Team Village) Tactic Table 4 - [Map](#)

Description:

Every operator makes the same call dozens of times an engagement: I need to do X, so how do I do it? Drop a binary, load a BOF, tunnel Impacket, abuse a LOLBIN? Today that runs on gut feel, and guessing wrong is how you get caught.

Praetor is an open-source, AI-driven OPSEC assistant that plugs into Empire and turns that call into an informed one. You tell it what you want to do, and it suggests the ways to do it, ranked by how much each one would expose, with a plain-language explanation of why one path is quieter than another.

AI is what makes the suggestions usable. It reads your intent in natural language, assembles the candidate techniques, ranks them, and writes the reasoning a senior operator would give you, putting tradecraft that normally lives in a few people's heads at every operator's fingertips. When you reach for a louder option than you need, it speaks up with a specific reason and a quieter alternative, not a blanket warning.

The advice is grounded, not guessed. Praetor cannot see the target's telemetry, so it never claims anything is "safe." It models the detection surface each technique exposes, ranks the options against each other, and bases those judgments on footprints measured in an instrumented range rather than on a model's intuition. You set the defensive posture you believe you are facing, and the suggestions adjust to it.

We will demo it live and let people use it against Empire: state an intent, see the AI-ranked options with their reasoning, and watch the confirmation gate fire when a choice is louder than it needs to be.

Access to a TryHackMe configured lab will be provisioned.

Speakers: Andrea Brosio, Ariz Soriano

SpeakerBio: Andrea Brosio

Andrea Brosio is a Security Researcher and Senior Content Engineer at TryHackMe, specializing in red teaming, malware development, and offensive security. With prior experience as a Bug Hunter and Red Team Operator he combines real-world adversarial expertise with a passion for creating engaging cybersecurity training.

SpeakerBio: Ariz Soriano, Associate Director - Red Team Operations @ THEOS Cyber Solutions

Ariz Soriano is Associate Director of Red Team at Theos, with nearly a decade of experience spanning Red Teaming, Penetration Testing, and Incident Response. He started his career on the defensive side, working as a SOC analyst and eventually leading SOC and IR teams for his first four years in the industry. That defensive foundation gives him a perspective most purely offensive operators don't have.

He built the Theos Red Team from the ground up, recruiting and training operators, designing red team infrastructure and tooling, and establishing the methodology and playbooks behind the team's APT simulation and purple teaming engagements. Today he runs a practice that delivers multiple concurrent engagements a year, balancing operations with presales, scoping, revenue targets, and people management.

Outside of client work, Ariz is passionate about building red team tooling, optimizing offensive workflows, and sharing knowledge with the community as a conference speaker. He also contributes to TryHackMe as a part-time Senior Content



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Precogly: Open-Source Threat Modeling for the AI-Coding Era

Tags: Intermediate | AppSec Village | Creator Event/Activity

When: Saturday, Aug 8, 11:30 - 12:30 PDT

Where: LVCCW Level 1 Hall 2 604 (Appsec Village) Arsenal - [Map](#)

Description:

AI agents are beginning to write larger parts of applications, from individual features to complete services. But if agents can build software, they also need a reliable way to threat model what they build.

Precogly is an open-source (Apache 2.0) OWASP project for repeatable, human-reviewable threat modeling in the AI-coding era. It uses structured, community-curated library packs that connect components, threats, and countermeasures to sources such as CWE, CAPEC, and compliance frameworks.

This gives AI agents guardrails. Instead of inventing threat models freely, they work off installed libraries, producing outputs that are easier to review, reproduce, and audit.

In this demo, attendees will see Precogly's DFD editor, library pack ecosystem, threat generation workflow, completion status dashboard, pack cross-checks for detecting untraced AI-generated items, and the OpenAPI REST API that agents can build on top of.

SpeakerBio: Vikramaditya Narayan

Vikramaditya Narayan is the creator of OWASP Precogly, an open-source, enterprise-grade threat modeling platform designed for repeatable, AI-agent-ready threat modeling. Previously, he designed the prototype for a YC-funded AI governance platform. Vikramaditya leads the Bangalore chapter of Threat Modeling Connect and has spoken at ThreatModCon DC on emergent risks in multi-agentic systems and at OWASP on using AI in threat modeling. He holds an MS from Carnegie Mellon and is a Certified Threat Modeling Professional.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Privacy You Inherit: How Cultural History Writes the Source Code for AI Surveillance Policy

Tags: Policy @ DEF CON | Creator Talk/Panel

When: Saturday, Aug 8, 12:30 - 13:30 PDT

Where: LVCCW Level 1 Hall 3 801 (Creator Stage 1) - [Map](#)

Description:

Privacy isn't a principle. It's an inheritance — and AI is accelerating past every inheritance at once. This talk traces four lived experiences with surveillance — post-Mao China's "watchful neighbor," Stasi-era Germany's distrust of the state, Soviet communal density's "everyone already knows," and an American market that traded a constitutional right to privacy for one-click convenience — and shows how each set the privacy floor people now expect from AI. Chinese citizens accept face-scans but punish commercial data sale. Germans push back on the tech itself. Russians shrug. Americans click accept and let 23andMe hand DNA to law enforcement. Then AI changes the game. ChatGPT logs surface kids who type the wrong thing. Flock cameras blanket neighborhoods "for the children." Clear sells your face for a faster TSA line. None of these systems sit cleanly inside any inherited default — and federal policy has gone quiet. Audience leaves with: a vocabulary for diagnosing whose privacy default an AI proposal is actually written for; the federal-vacuum / state-patchwork pattern; and three concrete asks — plain-language consent, a "kudos wall" for companies that earn trust, and abstraction-layer tools that read T&Cs for users.

SpeakerBio: Tati

Tatiana (or Tati) is a Technical Program Manager who spends their days breaking telcos (amongst other things), managing logistics and wrangling hackers. They have no formal policy credentials, and that's kind of the point. The grandchild of Holocaust survivors and the child of Soviet émigrés, Tatiana didn't learn about surveillance overreach in a classroom or a think tank. They learned it the way most people in their family did — through stories of what happens when the state decides it has a right to know everything about everyone. That inheritance is why they're here, talking policy at a hacker conference instead of leaving it to the people who usually do

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Privacy's Defender with Women in Security and Privacy (WISP)

Tags: Women in Security and Privacy (WISP) | Creator Talk/Panel

When: Saturday, Aug 8, 15:30 - 16:30 PDT

Where: LVCCW Level 1 Hall 4 1303 (Women in Security and Privacy (WISP) Community) - [Map](#)

Description:

Join WISP and EFF for a conversation featuring WISP Board Chair Alyssa Coley and former EFF Executive Director Cindy Cohn in discussion about Cindy's book: Privacy's Defender: My Thirty-Year Fight Against Digital Surveillance.

Cindy has spent three decades tangling with the feds, fighting for data security, and arguing in court to protect our access to science and knowledge on the internet. This is a rare chance to hear her story up close.

Speakers: Cindy Cohn, Alyssa Coley

SpeakerBio: Cindy Cohn, Executive Director at Electronic Frontier Foundation

Cindy Cohn is the Executive Director of the Electronic Frontier Foundation. From 2000-2015 she served as EFF's Legal Director as well as its General Counsel. Ms. Cohn first became involved with EFF in 1993, when EFF asked her to serve as the outside lead attorney in *Bernstein v. Dept. of Justice*, the successful First Amendment challenge to the U.S. export restrictions on cryptography. Ms. Cohn is the author of the professional memoir, called *Privacy's Defender* published by MIT Press in March, 2026. She is also the co-host of EFF's award-winning podcast, *How to Fix the Internet*.

--

Cohn first became involved with EFF in 1993, when EFF asked her to serve as the outside lead attorney in *Bernstein v. Dept. of Justice*, the successful First Amendment challenge to the U.S. export restrictions on cryptography. She served as EFF's Legal Director as well as its General Counsel from 2000 through 2015, and she has served as Executive Director since then. She also has co-hosted EFF's award-winning "How to Fix the Internet" podcast, which recently concluded its sixth season. Her professional memoir covering her time at EFF, *Privacy's Defender: My Thirty-Year Fight Against Digital Surveillance*, was published earlier this year by MIT Press.

SpeakerBio: Alyssa Coley, Privacy & Product Counsel at Scopely

Alyssa is on the Board of Women In Security and Privacy (WISP) and is Privacy & Product Counsel at Scopely. As in-house counsel, she focuses on integrating privacy by design into product development and ensuring global privacy compliance. Previously, she gained experience in privacy consulting and cybersecurity incident response. She has been involved with WISP for nearly a decade where she developed her interest in locksport and continues to further WISP's mission to advance women and underrepresented communities to lead the future of security and privacy.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Privacy's Defender: How Hackers Protected the Internet Before and Can Do It Again

Tags: Policy @ DEF CON | Creator Talk/Panel

When: Friday, Aug 7, 15:30 - 16:30 PDT

Where: LVCCW Level 1 Hall 3 801 (Creator Stage 1) - [Map](#)

Description:

EFF's Outgoing Executive Director Cindy Cohn presents her first-person stories from her recently published book, *Privacy's Defender*, that take you Inside the privacy battles that have shaped today's Internet. It includes the hackers who helped free up encryption technology from US governmental control, allowing us to have the still imperfect privacy and security we now have online, and the battles to stop the mass NSA spying and eternal gag orders that arose from the governments formerly secret mass spying programs in the aftermath of the 9/11 attacks. She then draws from that long career of legal activism to the fights of today and tomorrow, featuring the role that hackers can play in helping to bring about a better, more just future.

SpeakerBio: Cindy Cohn, Executive Director at Electronic Frontier Foundation

Cindy Cohn is the Executive Director of the Electronic Frontier Foundation. From 2000-2015 she served as EFF's Legal Director as well as its General Counsel. Ms. Cohn first became involved with EFF in 1993, when EFF asked her to serve as the outside lead attorney in *Bernstein v. Dept. of Justice*, the successful First Amendment challenge to the U.S. export restrictions on cryptography. Ms. Cohn is the author of the professional memoir, called *Privacy's Defender* published by MIT Press in March, 2026. She is also the co-host of EFF's award-winning podcast, *How to Fix the Internet*.

--

Cohn first became involved with EFF in 1993, when EFF asked her to serve as the outside lead attorney in *Bernstein v. Dept. of Justice*, the successful First Amendment challenge to the U.S. export restrictions on cryptography. She served as EFF's Legal Director as well as its General Counsel from 2000 through 2015, and she has served as Executive Director since then. She also has co-hosted EFF's award-winning "How to Fix the Internet" podcast, which recently concluded its sixth season. Her professional memoir covering her time at EFF, *Privacy's Defender: My Thirty-Year Fight Against Digital Surveillance*, was published earlier this year by MIT Press.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Noob Community - Friday - 11:00-11:30 PDT

Title: Privilege Escalation: A Career Story

Tags: Noob Community | Creator Talk/Panel

When: Friday, Aug 7, 11:00 - 11:30 PDT

Where: LVCCW Level 1 Hall 4 1417 (Noob Community) - [Map](#)

Description:

Nobody handed us a roadmap. Before cybersecurity, our backgrounds looked nothing like the industry expected.

This is for everyone who's ever lurked in Discord, watched a conference talk, or read a writeup from someone and thought, "I wish I could talk with them."

PROTIP: You can, and you should.

We will share our unfiltered stories of breaking into the industry from non-traditional paths. The imposter syndrome, the cold messages to people we idolized, and what happened when we suddenly stopped being afraid to ask.

We plan to invite well-known figures from the community to come in chat with everyone and do a little mini social chat where everyone can ask the questions to hopefully people they idolize!

Speakers:Ryan Bonner,Whit Taylor

SpeakerBio: Ryan Bonner, Lead Security Engineer at Arcanum Information Security

Ryan Bonner is a Lead Security Engineer at Arcanum Information Security, where he builds AI systems, hacks them, and runs application penetration tests. Off the clock he hunts wide-scope bug bounty programs.

SpeakerBio: Whit Taylor

No BIO available

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Privilege Escalation: Building a Cyber Career with Zero Support

Tags: Noob Community | Creator Talk/Panel

When: Saturday, Aug 8, 14:15 - 14:45 PDT

Where: LVCCW Level 1 Hall 4 1417 (Noob Community) - [Map](#)

Description:

Elevator Pitch I moved across the world to start a master's in cybersecurity with little technical knowledge and no local network. I did not just find a career; I engineered one from scratch. Today, I hold a Master's degree, multiple certifications, and advisory board seats at two distinct organizations. I started as a student who had to build her own village. My talk is a "noob-to-leader" blueprint for anyone starting at ground zero. I will show you how to cut through industry noise, take your first big initiative, and turn a lack of guidance into your greatest leadership strength.

Description Most people say that to succeed in cyber, you need a long list of certifications and years of coursework. But what do you do when you are starting with a blank slate and no one is there to guide you?

When I began my journey as an international student, I had no contacts, no prior experience, and no roadmap. I had to learn how to distinguish the "signal" of real opportunities from the overwhelming "noise" of opinions and entry-level gatekeeping.

I took ownership of my path. I jumped into hackathons, volunteered for professional organizations, and eventually became an advisor helping veterans translate their military service into civilian cyber careers. I discovered that leadership was the ultimate technical growth: guiding others forced me to master complex concepts deeper and faster than any individual study could. By supporting others in the field, I was not just building a network; I was validating and sharpening my own technical expertise. In addition to my corporate role, I serve on the advisory boards for a university serving veterans and the nation's first Microsoft Certified high school.

In this 30-minute session, I am sharing the "Bootstrap Protocol" I used to move from the classroom to the boardroom. We will cover:

- The Initialization Phase: How to use hackathons and student organizations as your personal technical laboratory.
- The Mentor Mindset: How helping veterans transition to civilian roles forced me to master the cybersecurity field faster.
- Building the Infrastructure: A step by step guide on founding a chapter when you feel like you are standing alone.
- Service as a Shortcut: Why advising boards and helping others is the fastest way to build your own technical authority.

This is a practical, zero-fluff roadmap for the self-guided learner. If you feel like you are walking this path alone, come learn how to build the village you have been looking for.

Key Takeaways

- Stop Waiting for Permission: Why starting your own group or initiative is the best credential a newcomer can have.
- Mission-First Leadership: Insights into how helping others accelerates your own professional and technical growth.
- Filter the Noise: How to choose the right initiatives that actually lead to a seat at the advisory table.
- The Roadmap Blueprint: A curated handout for attendees featuring active opportunities and platforms where beginners can start building their technical and leadership track record today.

SpeakerBio: Akanksha Raghvesh

No BIO available



Title: Proactive Malicious Package Defense

Tags: Intermediate | AppSec Village | Creator Event/Activity

When: Saturday, Aug 8, 15:15 - 16:15 PDT

Where: LVCCW Level 1 Hall 2 604 (Appsec Village) Arsenal - [Map](#)

Description:

Whole development orgs are still rawdogging npm and other package registries, despite the continued rise of supply chain attacks involving malware targeted at both developers and the organizations they work for. Check out open-source tooling that can contribute to proactive defense, using either open or vendor-proprietary data sets

SpeakerBio: Darren Meyer

Darren is a security research advocate and practitioner that has worked on every side of the AppSec world at some point in the past 20 years. He's passionate about making security work more accessible and less stressful.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Blacks In Cyber Village - Friday - 12:30-12:55 PDT

Title: Prompt Injection Detection in Large Language Models: Survey and Evaluation of Open Source Tools

Tags: Blacks In Cyber Village | Creator Talk/Panel

When: Friday, Aug 7, 12:30 - 12:55 PDT

Where: LVCCW Level 3 W322-W324 (BIC Village) - [Map](#)

Description:

Prompt injection attacks trick Large Language Models into bypassing safety controls, leaking sensitive data, or performing unauthorized actions. This survey examines five open-source detection tools, LlamaFirewall, Cybersecurity AI, LLM Guard, Promptfoo, and OpenAI Guardrails Python. Analyzing How do they identify and block these attacks. The tools use different strategies: pattern-matching classifier, semantic reasoning systems, layered defenses, and code analyzers. We tested LlamaFirewall's PromptGuard 2 on four datasets containing 52,240 samples. When it flagged something as attack (malicious prompt), it was accurate 87%' 100% of the time, but it only caught 40%' 73% of actual attacks. Accuracy ranged from 57% on realistic chatbot conversations to 85% on artificial test cases.

SpeakerBio: Yasmin Eady, Ph.D. Student, NC A&T State University

Yasmin Eady is a PhD student in Computer Science at North Carolina A&T State University whose research focuses on prompt injection detection in large language models. Her work explores the security risks introduced by LLM-powered systems and the evaluation of open-source tools for identifying prompt injection vulnerabilities. Yasmin began her academic journey at West Los Angeles College, where she earned an Associate of Arts degree in Mathematics, and later completed a Bachelor of Science in Applied Mathematics at North Carolina A&T State University. Her broader research background includes cybersecurity, trust in distributed and social network systems, and biometric authentication.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Prompt Injection: Attacking and Defending AI-Powered Applications

Tags: AppSec Village | Creator Workshop | All Audiences

When: Saturday, Aug 8, 10:15 - 12:59 PDT

Where: LVCCW Level 1 Hall 2 604 (Appsec Village) Classroom - [Map](#)

Description:

Prompt injection has rapidly emerged as one of the most critical and least understood vulnerabilities in modern application security. As organizations race to integrate LLMs into customer-facing products, internal tools, and autonomous agents, attackers are already exploiting these systems in ways traditional security controls were never designed to catch. This one-day, hands-on training gives attendees a thorough, practical understanding of prompt injection — from basic chatbot manipulation to sophisticated attacks against RAG pipelines and autonomous AI agents. Using a purpose-built lab environment, attendees will exploit real vulnerabilities in LLM-powered applications, understand exactly why they work, and then build effective defenses against them. The course is structured as an attack-first, defend-second journey. By experiencing these vulnerabilities as an attacker, attendees leave with deep intuition about where AI systems.

SpeakerBio: Mohammed Ilyas Ahmed

I am a seasoned security and DevSecOps professional with deep expertise in helping organizations strengthen their security posture across modern, cloud-native environments.

I am an active contributor to the global technology community and a frequent speaker at leading industry conferences and platforms, including DEF CON, Black Hat, KubeCon (Paris), ISACA, IANS, and Wallarm, among others. I am also regularly invited to serve as a technical session judge.

publishing work that advances discussions around modern security practices, governance, and risk management. I am also a distinguished member of the Harvard Business Review Advisory Council.

My work has a global reach through my role as a Member of the Global Advisory Board at VigiTrust Limited (Dublin, Ireland).

I am the author of Cloud-Native DevOps, a practical guide to building scalable, reliable, and secure cloud-native applications.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: PromptPwn: Finding and Exploiting AI-Generated Vulnerabilities at Scale

Tags: AI | DEF CON Demo Labs | Intermediate | AppSec | Defense/Blue Team | DevOps | Offense/Red Team | Purple Team | DEF CON Demo Labs

When: Saturday, Aug 8, 14:00 - 14:45 PDT

Where: LVCCW Level 1 Hall 3 901 (Demo Labs Track 5) - [Map](#)

Description:

AI-assisted development tools don't just introduce vulnerabilities; they introduce the same vulnerabilities repeatedly.

PromptPwn is a tool designed to identify, track, and exploit common insecure patterns found in AI-generated code. It maintains a database of known vulnerability patterns produced by popular "vibe coding" workflows and provides scanning capabilities to detect these issues in real applications.

In this demo, we show how PromptPwn identifies vulnerable patterns such as injection flaws, authentication weaknesses, and insecure defaults across generated code. We demonstrate how these patterns can be exploited in practice, highlighting how repeatability makes them especially valuable from an attacker's perspective.

We also explore how prompt variations influence these outcomes and show how insecure patterns can be remediated by adjusting prompts, closing the loop between generation, exploitation, and correction.

This session focuses on practical demonstrations of how AI-generated code fails in predictable ways, and how those failures can be identified and abused at scale.

SpeakerBio: Georgia Weidman

Georgia Weidman is an offensive security researcher and author focused on breaking real-world systems. She wrote *Penetration Testing: A Hands-On Introduction to Hacking*, a practical guide used by students and practitioners to learn exploitation techniques.

Her work centers on how modern systems fail under attack, from mobile and IoT to enterprise environments. As a DARPA Cyber Fast Track performer, she developed the Smartphone Pentest Framework (SPF), a platform for mobile exploitation research.

She has conducted penetration tests, built exploitation tooling, and developed attack chains across multiple domains. Her approach prioritizes hands-on techniques over theory, demonstrating how assumptions about security break down in practice.

Georgia has presented internationally at conferences including Black Hat and DEF CON, with a focus on showing how things actually get hacked.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: PromptPwn: Finding and Exploiting AI-Generated Vulnerabilities at Scale

Tags: AI | DEF CON Demo Labs | Intermediate | AppSec | Defense/Blue Team | DevOps | Offense/Red Team | Purple Team | DEF CON Demo Labs

When: Friday, Aug 7, 10:00 - 10:45 PDT

Where: LVCCW Level 1 Hall 3 901 (Demo Labs Track 5) - [Map](#)

Description:

AI-assisted development tools don't just introduce vulnerabilities; they introduce the same vulnerabilities repeatedly.

PromptPwn is a tool designed to identify, track, and exploit common insecure patterns found in AI-generated code. It maintains a database of known vulnerability patterns produced by popular "vibe coding" workflows and provides scanning capabilities to detect these issues in real applications.

In this demo, we show how PromptPwn identifies vulnerable patterns such as injection flaws, authentication weaknesses, and insecure defaults across generated code. We demonstrate how these patterns can be exploited in practice, highlighting how repeatability makes them especially valuable from an attacker's perspective.

We also explore how prompt variations influence these outcomes and show how insecure patterns can be remediated by adjusting prompts, closing the loop between generation, exploitation, and correction.

This session focuses on practical demonstrations of how AI-generated code fails in predictable ways, and how those failures can be identified and abused at scale.

SpeakerBio: Georgia Weidman

Georgia Weidman is an offensive security researcher and author focused on breaking real-world systems. She wrote *Penetration Testing: A Hands-On Introduction to Hacking*, a practical guide used by students and practitioners to learn exploitation techniques.

Her work centers on how modern systems fail under attack, from mobile and IoT to enterprise environments. As a DARPA Cyber Fast Track performer, she developed the Smartphone Pentest Framework (SPF), a platform for mobile exploitation research.

She has conducted penetration tests, built exploitation tooling, and developed attack chains across multiple domains. Her approach prioritizes hands-on techniques over theory, demonstrating how assumptions about security break down in practice.

Georgia has presented internationally at conferences including Black Hat and DEF CON, with a focus on showing how things actually get hacked.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Telecom Village - Friday - 14:15-14:59 PDT

Title: Protecting Humans at Machine Speed - Engineering AI to Stop Spam, Scams & Digital Fraud at Telecom Scale

Tags: Telecom Village | Creator Talk/Panel

When: Friday, Aug 7, 14:15 - 14:59 PDT

Where: LVCCW Level 3 W321 (Telecom Village) - [Map](#)

Description:

1. What does it take to protect billions of daily calls, SMS, data sessions, and digital interactions across one of the world's largest and the second-largest telecom operator by subscriber base?
2. This talk explores how AI is transforming telecom networks from passive transport infrastructure into active security platforms capable of detecting, correlating, and disrupting spam, scams, malicious links, OTP abuse, and digital fraud before they reach customers.

SpeakerBio: Arvind Singh

No BIO available

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Contests - Friday - 13:00-14:59 PDT

Title: Pub Quiz at DEF CON

Tags: Pub Quiz at DEF CON | Contest

When: Friday, Aug 7, 13:00 - 14:59 PDT

Where: LVCCW Level 3 W327 (Misc Meeting Room) - [Map](#)

Description:

We're back with another Pub Quiz at DEF CON! After 4 very successful years hosting this event, we've made some improvements to make it even better. So... do you like pub quizzes? If so, get your butts over and join us for the 5th Pub Quiz at DEF CON 34.

The quiz will consist of 7 rounds, covering topics like '90s/2000s TV and movies, DEF CON trivia, music, cartoons, and yes, a little bit of sex. The theme is all the things that make DEF CON attendees exceptional, so there will truly be something for everyone. Expect a mix of visual rounds, audio rounds, and classic con questions. We need to keep you peeps stimulated.

This is a social event, so we encourage teams of 5–6 people. You never know... you might even meet the love of your life.

Did we mention CASH? That's right; cold, hard cash prizes for 1st, 2nd, and 3rd place teams. And as always, if there's a tie, we'll break it with a good old-fashioned dance-off, judged by the hosts and a few trusted goons.

Come for the trivia. Stay for the chaos.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Publicly Auditable Elections

Tags: Voting Village | Creator Talk/Panel

When: Friday, Aug 7, 13:30 - 13:59 PDT

Where: LVCCW Level 2 W220 (Voting Village) (Voting Village Talks) - [Map](#)

Description:

Distrust in the integrity of elections has become widespread in the U.S. and elsewhere. We ask voters to “trust the process” without giving voters any direct evidence that their votes have been correctly counted. Technology has existed for over forty years that allows voters and observers to independently verify the accuracy of election results without having to trust any election software, hardware, or personnel. This technology, which has come to be known as end-to-end verifiability, allows a verifiable election record to be published. Voters can use this record to confirm that their selections have been accurately included, and anyone can use this record to confirm that the included votes have been accurately tallied – all without compromising voter privacy or enabling coercion or vote-selling.

This talk will explain how end-to-end verifiability works as well as how and where it has been used in practice. It will also explore some recent advances which greatly simplify the processes of building the tools to enable verifiability, administering elections using these tools, and verifying the integrity of election results.

End-to-end verifiability offers a fundamental shift from trust-based elections to evidence-based elections, providing voters, candidates, journalists, and observers with independent means to confirm the accuracy of reported election outcomes.

SpeakerBio: Josh Benaloh

Josh Benaloh is the Senior Principal Cryptographer at Microsoft Research and an Affiliate Professor at the University of Washington's Paul G. Allen School of Computer Science & Engineering. He is an author of the 2018 National Academy of Sciences report "Securing the Vote: Protecting American Democracy" and has testified before Congress on verifiable election technologies. His work has been featured in publications including The New Yorker and WIRED. Dr. Benaloh holds an S.B. degree from the Massachusetts Institute of Technology and M.S., M. Phil., and Ph.D. degrees from Yale University. He served seventeen years on the Board of Directors of the International Association for Cryptologic Research and currently serves on the Coordinating Committee of the Election Verification Network which he chaired from 2020-2024. Outside of professional activities, Dr. Benaloh served eight years on and chaired the Citizen Oversight Panel for Sound Transit which is investing \$2 billion annually on expanding the public transit infrastructure for the Seattle region. He has also authored numerous puzzles for competitive puzzle-solving events.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Pulling Back the Curtain on the Voting Booth

Tags: Voting Village | Creator Talk/Panel

When: Saturday, Aug 8, 13:30 - 13:59 PDT

Where: LVCCW Level 2 W220 (Voting Village) (Voting Village Talks) - [Map](#)

Description:

This presentation by Max Springer (postdoctoral research fellow, Princeton University Center for Information Technology Policy) and Marilyn Marks (Coalition for Good Governance) presents unsettling new findings that escalate the danger of a known, unpatched vulnerability in Dominion Voting Systems version used in Georgia and multiple other jurisdictions. First disclosed in 2022 by University of Michigan and Auburn University researchers, the flaw allows cast-vote records and ballot images to be "unshuffled," revealing the order in which ballots were cast, and, when combined with public information like scanner logs, scanner public counters, poll books check-in files, or timestamped polling place video, exposing how specific individuals voted. Georgia and many affected jurisdictions have taken no corrective action despite the software patch offered by Dominion in late 2022.

Springer and Marks demonstrate that these exploits, once assumed to require sophisticated programming skills, can now be carried out by almost anyone. Using only publicly available Georgia election records and off-the-shelf AI tools, and without writing custom code, the presenters demonstrate the ready ability to determine how a substantial share of Georgia voters cast their ballots in the contentious May 2026 primary.

The findings arrive at a pivotal moment: Georgia election officials are currently divided over whether to require a security patch bringing ballot scanners into compliance with the state's secret-ballot guarantee. Some officials resist any change and instead push to conceal the underlying public records, preserving insiders' access to voter-choice data while leaving the public without elections oversight and verification rights.

Springer and Marks argue that AI has fundamentally lowered the barrier to exploiting this flaw, transforming a theoretical privacy risk into an urgent, practical threat to the secret ballot in multiple jurisdictions. They call for mandatory patching and warn that inaction before the 2026 midterms could compromise the constitutional right to a private vote for millions of Americans.

Speakers: Marilyn Marks, Max Springer

SpeakerBio: Marilyn Marks

Marilyn Marks is Executive Director of the Coalition for Good Governance, a nonpartisan nonprofit working to strengthen election security and protect the right to a secret ballot. For more than 17 years she has focused on improving the technology used in U.S. elections, especially in Georgia. Her group is behind *Curling v. Raffensperger*, a landmark federal case challenging the security of touchscreen voting machines. Georgia is using a second generation of touchscreen voting machines, with flawed software that Marks and many cybersecurity experts fear may be used to disrupt target state Georgia's elections this year.

SpeakerBio: Max Springer

Max Springer is an algorithms researcher, science communicator, and tech policy consultant. Currently, he is a postdoctoral research fellow at Princeton University. He earned his PhD from the University of Maryland under MohammadTaghi Hajiaghayi, with support from an NSF Graduate Research Fellowship. His dissertation, "The Price of Fairness in Algorithmic Decision Making", developed approximation algorithms with fairness and reliability guarantees—an agenda he now extends from classical machine-learning problems to modern AI systems. He has conducted research at Google, Nokia Bell Labs, Yale, and the Max Planck Institute, and received Bell Labs' Outstanding Innovation Award. Beyond research, he contributed

to a recent United Nations report on AI and works with policymakers on responsible algorithmic deployment, including election systems



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: PurpleLoop: Closing the Loop Between Detection Rules, Log Schemas, and Purple-Team Validation

Tags: Demo | Cloud Village | Creator Talk/Panel

When: Friday, Aug 7, 12:50 - 13:20 PDT

Where: LVCCW Level 3 W313 (Cloud Village Talks) - [Map](#)

Description:

The problem Sentinel deployments rot. Mid-market SOC's run 80 to 300 analytics rules, and a large share haven't fired a true positive in 90 days. Many reference tables or columns that don't exist in the tenant because the rule was copied from a Microsoft post written for a different topology. The public Azure-Sentinel repo ships new content weekly and almost nobody reconciles against it. One layer deeper, Log Analytics ingests 20 to 80 tables per tenant, and most teams have never audited which have any coverage and which are dark. And almost nobody validates that the rules they do have actually fire against the techniques they claim to cover.

What PurpleLoop is PurpleLoop is an LLM-augmented detection-engineering workflow built on one insight: rule authoring, coverage analysis, and purple-team validation are the same job, and they should be one tool. It does four things, none individually novel, never previously combined into one workflow:

- Reviews deployed rules by diffing against the live Azure-Sentinel repo and community libraries, flagging drift, dead operators, missing siblings.
- Suggests new rules from your actual workspace schema, not Microsoft's reference topology. A rule needing DeviceProcessEvents isn't suggested if MDE isn't onboarded.
- Generates purple-team scenarios and validates rules against them. The tool runs an atomic-style simulation, checks whether the rule fires, and patches the KQL if it doesn't. The loop closes itself.
- Builds a detection-gap map that distinguishes "no rule for this" from "no telemetry for this." Most coverage tools miss the second category.

Why an LLM The LLM provides the connective reasoning between the pieces. It is not in the codegen path. PurpleLoop reasons in a Sigma-inspired intermediate detection representation (IDR), and a deterministic compiler renders to KQL. The queries that run on your workspace are produced by code we wrote, not by pattern completion. Hallucinated columns and invented operators are eliminated at the compiler boundary, not at the prompt boundary.

What attendees take home A working open-source tool installable in minutes, a reusable methodology not bound to Sentinel, and prompt-engineering patterns for security workflows where correctness matters. The talk argues the case, demos the tool live against a real tenant, and hands the code to the room.

SpeakerBio: Ariz Soriano, Associate Director - Red Team Operations @ THEOS Cyber Solutions

Ariz Soriano is Associate Director of Red Team at Theos, with nearly a decade of experience spanning Red Teaming, Penetration Testing, and Incident Response. He started his career on the defensive side, working as a SOC analyst and eventually leading SOC and IR teams for his first four years in the industry. That defensive foundation gives him a perspective most purely offensive operators don't have.

He built the Theos Red Team from the ground up, recruiting and training operators, designing red team infrastructure and tooling, and establishing the methodology and playbooks behind the team's APT simulation and purple teaming engagements. Today he runs a practice that delivers multiple concurrent engagements a year, balancing operations with presales, scoping, revenue targets, and people management.

Outside of client work, Ariz is passionate about building red team tooling, optimizing offensive workflows, and sharing knowledge with the community as a conference speaker. He also contributes to TryHackMe as a part-time Senior Content Engineer, creating hands-on cybersecurity labs and challenges based on real-world attack techniques.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Contests - Saturday - 10:00-17:59 PDT

Title: PWN UR H0M3 - DDoS CTF

Tags: DDoS Contest | Contest

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 307 (DDoS Contest) - [Map](#)

Description:

A chaotic DDoS-themed CTF where sketchy devices, busted services, weird signals, and sneaky clues are begging to be owned. Scan the network, break IoT devices, decode the nonsense, and prove you can pwn your home before your home pwns you. This CTF is designed to help you learn about the cutting edge in DDoS attacks and defense. We also have an IoT lab of devices hacked and infected with botnet malware that you can play around with. Beginners welcome. We have some fabulous prizes including gift cards donated from Hak5 so please check it out!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Contests - Friday - 10:00-17:59 PDT

Title: PWN UR H0M3 - DDoS CTF

Tags: DDoS Contest | Contest

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 307 (DDoS Contest) - [Map](#)

Description:

A chaotic DDoS-themed CTF where sketchy devices, busted services, weird signals, and sneaky clues are begging to be owned. Scan the network, break IoT devices, decode the nonsense, and prove you can pwn your home before your home pwns you. This CTF is designed to help you learn about the cutting edge in DDoS attacks and defense. We also have an IoT lab of devices hacked and infected with botnet malware that you can play around with. Beginners welcome. We have some fabulous prizes including gift cards donated from Hak5 so please check it out!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Contests - Sunday - 10:00-11:59 PDT

Title: PWN UR H0M3 - DDoS CTF

Tags: DDoS Contest | Contest

When: Sunday, Aug 9, 10:00 - 11:59 PDT

Where: LVCCW Level 1 Hall 1 307 (DDoS Contest) - [Map](#)

Description:

A chaotic DDoS-themed CTF where sketchy devices, busted services, weird signals, and sneaky clues are begging to be owned. Scan the network, break IoT devices, decode the nonsense, and prove you can pwn your home before your home pwns you. This CTF is designed to help you learn about the cutting edge in DDoS attacks and defense. We also have an IoT lab of devices hacked and infected with botnet malware that you can play around with. Beginners welcome. We have some fabulous prizes including gift cards donated from Hak5 so please check it out!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Contests - Sunday - 12:00-12:59 PDT

Title: PWN UR H0M3 DDoS CTF Winner Announcements

Tags: DDoS Contest | Contest

When: Sunday, Aug 9, 12:00 - 12:59 PDT

Where: LVCCW Level 1 Hall 1 307 (DDoS Contest) - [Map](#)

Description:

PWN UR H0M3 DDoS CTF winners announced and prizes handed out.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Pwning Agentic Browsers with PleaseFix: A New Vulnerability Class for 0-Click Takeover

Tags: AI Village | Creator Talk/Panel

When: Sunday, Aug 9, 12:00 - 12:30 PDT

Where: LVCCW Level 1 Hall 3 1105 (Creator Stage 3) - [Map](#)

Description:

Every major AI lab now ships an agentic browser: ChatGPT Atlas, Perplexity Comet, Claude in Chrome, Gemini in Chrome, and Microsoft Copilot Actions. To make them work, vendors intentionally relax thirty years of browser security. Atlas loosens Same-Origin Policy, Gemini and Edge add localhost access, Comet opens the filesystem, and Claude runs scripts on any site. The main defense is model safety training. These are design choices, not bugs, reviving XSS, sandbox escapes, and drive-by exploitation.

We ran the first cross-platform analysis of all five. We introduce PleaseFix, a new agent-targeting vulnerability class (the evolution of ClickFix), exploited via Intent Collision, which merges attacker content with the user's request into one plan the agent cannot untangle. We also present HistoryFixing, which weaponizes a function shipped in every browser since 2008 to poison the browsing history agents trust as ground truth.

Walk up to learn the agentic-browser threat model, the vulnerabilities, and which were agent-specific versus consistent across all five. You will see how we chained Intent Collision and HistoryFixing, from zero-click vectors (poisoned tweet, calendar invite), to conduct RCE, reverse shells, data exfiltration and poisoning, filesystem theft, account takeovers (Slack, X, 1Password, Claude), rogue actions on MFA-gated sites, unauthorized Amazon purchases, malicious collaborators added to your private enterprise GitHub, and more. We link videos of every attack. We break down the soft versus hard boundaries each vendor built, what failed and what held: only deterministic, code-level defenses stopped us. All findings responsibly disclosed.

SpeakerBio: Stav Cohen

Stav Cohen is an AI Security Research Lead at Zenity and a PhD student at the Technion, Israel Institute of Technology. His research focuses on breaking, and then fixing, AI agents, spanning security vulnerabilities across agentic AI systems, LLM-powered applications, and enterprise AI platforms. He discovers new attack vectors, develops remediation strategies, and works to drive the industry toward stronger security practices. His offensive security work spans attacks on RAG pipelines, multi-agent delegation protocols, agentic browsers, and production-scale GenAI systems. He introduced the concept of Promptware: a new class of inference-time threats that exploit GenAI models through malicious prompts, turning them from helpful assistants into tools for data exfiltration, lateral movement, and even physical-world consequences. He presents his findings at leading security venues across the world. His PhD research focuses on the secure integration of Generative AI into real-world infrastructure, particularly Cyber-Physical-Human Systems involving human-in-the-loop interactions, such as smart water networks and GenAI-powered virtual assistants. He explores how GenAI agents can be safely and effectively integrated into these environments to support real-time decision-making, anomaly detection, and human-machine collaboration. He is also a thought leader in the AI security space, sharing knowledge through conference talks, blog posts, and community engagement.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Pwning Rekordbox: Unauthenticated filesystem access in the world's most popular DJ software

Tags: DEF CON Official Talk | Exploit

When: Friday, Aug 7, 15:00 - 15:30 PDT

Where: LVCCW Level 1 Hall 3 904 (Main Track 4) - [Map](#)

Description:

First public disclosure. rekordbox, the world's most popular DJ software, silently runs an NFS server whenever you play over the network, and it shares your whole hard drive, not just your music. Any device on the same subnet can quietly read your SSH keys, passwords, and files. It works the same on Windows, macOS, iOS, and Android. The catch: the obvious fix would break 20 years of hardware compatibility.

This talk breaks down the PRO DJ LINK protocol, shows how any device on the wire talks its way into full filesystem access, and explains why the fix is stranger than it looks.

- CWE-284: Improper Access Control: <https://cwe.mitre.org/data/definitions/284.html>
- Deep Symmetry, crate-digger (Java, Pro DJ Link NFS client): <https://github.com/Deep-Symmetry/crate-digger>
- EvanPurkhiser, prolink-connect (TypeScript, Pro DJ Link library): <https://github.com/EvanPurkhiser/prolink-connect>
- Deep Symmetry, DJ Link Packet Analysis: <https://djl-analysis.deepsymmetry.org/>
- CVSS v3.1 Calculator: <https://www.first.org/cvss/calculator/3.1>
- JPCERT/CC Vulnerability Coordination: <https://www.jpccert.or.jp/english/vh/report.html>
- Digital DJ Tips, Global DJ Census / AlphaTheta market share:
<https://www.digitaldjtips.com/pioneer-alphatheta-industry-standard/>

SpeakerBio: Christopher "TRIODE" Le

TRIODE is an engineer, semi-professional DJ, and livestreamer who has performed at the last four Defcons. He discovered this vulnerability while reverse-engineering the Pro DJ Link protocol to build custom performance tooling. His background spans systems programming and network protocol analysis. This is his first Defcon talk submission.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Pwning the Internet of Agents: Zero-Click Backdoors in OpenClaw and a Global Agent Botnet on MoltBook

Tags: AI Village | Creator Talk/Panel

When: Friday, Aug 7, 15:00 - 15:59 PDT

Where: LVCCW Level 1 Hall 2 603 (AI Village) - [Map](#)

Description:

This is a sit down discussion in a more casual conversational format: Always-on agents like OpenClaw now live in your chat, browser, and Google Workspace and act with your permissions. They swallow untrusted content with no wall between it and your intent, trusting the model's vibes to tell data from orders. MoltBook, the self-proclaimed "Internet of Agents," pipes thousands of these agents into one feed they reread every 30 minutes. What could go wrong?

We attacked the node and the network. On a single agent, a zero-click prompt injection buried in a shared doc backdoors OpenClaw into adding an attacker-owned chat integration, no exploit, no CVE, then runs commands, steals and wipes files, persists by rewriting the agent's SOUL.md on a timer, and drops a Sliver C2 for full host takeover. On the network, we reverse-engineered MoltBook, tore through the hype, and crafted posts that prompt-inject agents into following our link, then mapped where they phoned home from. Over 1,000 agents in 70+ countries took the bait, others reposted our content on their own, and we stopped at a harmless ping, though the same trick ships a worm.

Walk up to learn who actually lives on this "thriving agent society," plotted across the globe: a sliver of the hype, heavy on human-run bots, crypto spam, and a ranking algorithm so broken the same posts squat on top for weeks. You will see the one-agent kill chain from injection to RCE and host takeover, and why only a hard, code-level boundary, not alignment, would have stopped us.

Speakers: João Maria Campos Donato, Stav Cohen

SpeakerBio: João Maria Campos Donato

João Maria Campos Donato is an AI security researcher specializing in red teaming and adversarial evaluation of AI systems. He holds an MSc in Informatics Security. He currently works as an AI Red Team Researcher at Zenity and as an AI Red Team Operator at BT6, where he identifies vulnerabilities in AI systems and helps organizations mitigate emerging risks related to model misuse, prompt injection, and system-level failures.

SpeakerBio: Stav Cohen

Stav Cohen is an AI Security Research Lead at Zenity and a PhD student at the Technion, Israel Institute of Technology. His research focuses on breaking, and then fixing, AI agents, spanning security vulnerabilities across agentic AI systems, LLM-powered applications, and enterprise AI platforms. He discovers new attack vectors, develops remediation strategies, and works to drive the industry toward stronger security practices. His offensive security work spans attacks on RAG pipelines, multi-agent delegation protocols, agentic browsers, and production-scale GenAI systems. He introduced the concept of Promptware: a new class of inference-time threats that exploit GenAI models through malicious prompts, turning them from helpful assistants into tools for data exfiltration, lateral movement, and even physical-world consequences. He presents his findings at leading security venues across the world. His PhD research focuses on the secure integration of Generative AI into real-world infrastructure, particularly Cyber-Physical-Human Systems involving human-in-the-loop interactions, such as smart water networks and GenAI-powered virtual assistants. He explores how GenAI agents can be safely and effectively integrated into these environments to support real-time decision-making, anomaly detection, and human-machine collaboration. He is also a thought leader in the AI security space, sharing knowledge through conference talks, blog posts, and community engagement.



Title: pymsi: Interactive MSI Installer Analysis in Python and the Browser

Tags: Intro/Beginner | DEF CON Demo Labs | AppSec | Defense/Blue Team | Malware | Threat Intel/Hunting | DEF CON Demo Labs

When: Friday, Aug 7, 15:00 - 15:45 PDT

Where: LVCCW Level 1 Hall 3 902 (Demo Labs Track 6) - [Map](#)

Description:

pymsi is a pure-Python library for parsing, analyzing, and extracting files from Windows installer (MSI) packages, without relying on native Windows APIs or tooling. It provides direct access to MSI database tables, embedded binary streams, and installer metadata, enabling security researchers to inspect installer behavior and extract files from MSI installers.

We will demonstrate its ability to safely tear apart malicious MSI droppers, dump internal database tables, and extract embedded payloads without risking accidental execution. Attendees will see how the CLI and Python API can be used to triage files and integrate it into automated analysis pipelines, including how it has been integrated into other open source tools to extract embedded payloads and identify malicious CustomAction behaviors.

Because it is written entirely in Python, it runs seamlessly on any OS with a Python interpreter, including web browsers. The demo will showcase the online MSI viewer, a client-side tool powered by Pyodide that gives pymsi a familiar lessmsi-style UI for working with MSI installers from any device with a web browser. Demos will also show new security analysis features for identifying suspicious installer behaviors and inspecting contents of embedded binary streams within a browser.

SpeakerBio: Ryan "Nightlark" Mast

Ryan is a software engineer working on open source projects to make the electric grid more reliable. His interests include software security, niche video games, tearing apart "smart" devices, and reverse engineering audio/video hardware used in live productions.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: pymsi: Interactive MSI Installer Analysis in Python and the Browser

Tags: Intro/Beginner | DEF CON Demo Labs | AppSec | Defense/Blue Team | Malware | Threat Intel/Hunting | DEF CON Demo Labs

When: Saturday, Aug 8, 11:00 - 11:45 PDT

Where: LVCCW Level 1 Hall 3 902 (Demo Labs Track 6) - [Map](#)

Description:

pymsi is a pure-Python library for parsing, analyzing, and extracting files from Windows installer (MSI) packages, without relying on native Windows APIs or tooling. It provides direct access to MSI database tables, embedded binary streams, and installer metadata, enabling security researchers to inspect installer behavior and extract files from MSI installers.

We will demonstrate its ability to safely tear apart malicious MSI droppers, dump internal database tables, and extract embedded payloads without risking accidental execution. Attendees will see how the CLI and Python API can be used to triage files and integrate it into automated analysis pipelines, including how it has been integrated into other open source tools to extract embedded payloads and identify malicious CustomAction behaviors.

Because it is written entirely in Python, it runs seamlessly on any OS with a Python interpreter, including web browsers. The demo will showcase the online MSI viewer, a client-side tool powered by Pyodide that gives pymsi a familiar lessmsi-style UI for working with MSI installers from any device with a web browser. Demos will also show new security analysis features for identifying suspicious installer behaviors and inspecting contents of embedded binary streams within a browser.

SpeakerBio: Ryan "Nightlark" Mast

Ryan is a software engineer working on open source projects to make the electric grid more reliable. His interests include software security, niche video games, tearing apart "smart" devices, and reverse engineering audio/video hardware used in live productions.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Red Team Village - Saturday - 10:00-11:59 PDT

Title: Pyramid of Pain-Red Team (Human and Technical Friction)

Tags: Red Team Village | Misc

When: Saturday, Aug 8, 10:00 - 11:59 PDT

Where: LVCCW Level 1 Hall 1 309 (Red Team Village) Workshop Tactic Table 6 - [Map](#)

Description:

Inspired by the Pyramid of Pain, this session flips the lens inward to examine the friction Red Teams face across tools, policies, and organizational constraints. We will explore how limited scope, tool fatigue, and misaligned incentives reduce the real impact of security testing—and how to (possibly) fix it. Using frameworks such as MITRE ATT&CK, attendees will learn to prioritize findings by business risk, translate technical results into actionable outcomes, and build repeatable processes that drive remediation.

SpeakerBio: Frank Victory

Frank Victory is a seasoned cybersecurity leader with over 30 years of experience shaping impactful security strategies. Focused on results rather than titles, he has excelled in both technical and leadership roles, bringing deep expertise in defensive and offensive security—spanning blue and red team operations, incident response, and threat & risk management.

Passionate about developing the next generation of cybersecurity professionals, Frank teaches at local community colleges and leads instruction for CU Boulder's programs in Social Engineering, Ethical Hacking, DFIR, and Threat Hunting. As Vice President of the Denver OWASP chapter, he fosters community engagement through meetups and conferences, including SnowFROC.

Frank also co-hosts the Colorado=Security Podcast, where he interviews local cybersecurity professionals, delving into their journeys, challenges, and insights—always ending with the question: What is the biggest challenge in cybersecurity today?

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Q-Day - the Early Years...

Tags: Quantum Village | Creator Talk/Panel

When: Friday, Aug 7, 17:00 - 17:30 PDT

Where: LVCCW Level 1 Hall 3 1104 (Creator Stage 4) - [Map](#)

Description:

Everyone's obsessed with the Hollywood idea of a quantum computer cracking RSA-2048 in seconds. But the real Act One of Q-Day won't be anything like a rapid-fire decryption spree: click, click, quantum stuff, "I'm in!" It'll be quieter, meaner, and quite possibly have nothing to do with harvest-now, decrypt later (HNDL)! This talk breaks down what the actual opening moves look like. Think forgery before decryption and signatures before secrets. Also, cracking ~73 emails a year with a five-day Gidney-style attack is a far less realistic nightmare than "harvest now, decrypt everything." We'll first walk through the threat model hackers actually need to care about. Then we'll cut to another nightmare scenario. Bitcoin. Because if any technology needs a Quantum Hail Mary, it's blockchain. Spoiler: Bitcoin won't be ready by Q-Day. Join Konstantinos Karagiannis (@KonstantHacker) for a blockbuster treatment on where quantum attacks will start and who will get hit first. It's not the apocalypse you were promised. It's worse.

SpeakerBio: Konstantinos Karagiannis, Protiviti

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Q&A with the "How to Profile an entire C-suite in 10 days" speaker

Tags: OSINT For Good Community | Creator Event/Activity

When: Sunday, Aug 9, 11:00 - 11:15 PDT

Where: LVCCW Level 1 Hall 4 1307 (OSINT4Good Community) - [Map](#)

Description:

Stop by and chat with Sarah Muriel the speaker on How to Profile and Entire C-Suite in 10 days.

SpeakerBio: Sarah Muriel, Bishop Fox

Sarah Muriel is an Intelligence Analyst from Mexico with more than 6 years of experience in open source investigations, currently working with the Attack Surfaces of companies all over the world. In her spare time she likes participating in various international OSINT related CTFs and developing retro-style websites. She's also fairly active in the cybersecurity community, being part of the organization team for one of Mexico's top conferences.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

OSINT For Good Community - Friday - 14:30-14:59 PDT

Title: Q&A with the Classical OSINT Using AI speaker

Tags: OSINT For Good Community | Creator Event/Activity

When: Friday, Aug 7, 14:30 - 14:59 PDT

Where: LVCCW Level 1 Hall 4 1307 (OSINT4Good Community) Stage - [Map](#)

Description:

Stop by and chat with reconcerto, the speaker on Classical OSINT using AI (Actual Intelligence)

SpeakerBio: Bianca C. Ionescu/reconcerto

Bianca Ionescu is a CyberCorps SFS scholar pursuing a master's degree in cybersecurity at UNLV. She's served as a leader within cybersecurity student organizations, promoting growth, inclusion, and professional development. Her interests include open-source intelligence and mentoring new learners entering the field. Offline, she enjoys strength training and playing the viola. She's motivated by community building, continuous learning, and the challenge of solving complex security problems that inspire her growth and resilience every day.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Q&A with the OSINT4Good Panel

Tags: OSINT For Good Community | Creator Event/Activity

When: Friday, Aug 7, 11:00 - 11:30 PDT

Where: LVCCW Level 1 Hall 4 1307 (OSINT4Good Community) Stage - [Map](#)

Description:

Stop by and chat with the panelists from the OSINT4Good panel.

Speakers: Angela Ramos, Kenny J, Brent Louie

SpeakerBio: Angela Ramos, University of Tampa

Angela Ramos is a University of Tampa cybersecurity lecturer. She leads the Scam Busters student program, coaches Trace Labs Search Party CTFs, and volunteers with US Cyber Games. She holds the GCIH, GSLC, and CEH certifications and spent a decade in DoD cyber operations.

SpeakerBio: Kenny J, Trace Labs

Senior Infrastructure Engineer by day. Osint for Good by night. His is the only Trace Labs coach to have coached 20+ CTFs, earning him the singular rank of Legendary Coach.

SpeakerBio: Brent Louie, Reporting Team Lead at Trace Labs

Brent Louie is the Reporting Team Lead at Trace Labs and an Associate Director of Data Science with more than 15 years of experience in the biotechnology industry. He focuses on applying OSINT methodologies to missing persons investigations and helping transform crowdsourced research into actionable investigative leads for law enforcement.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Quality over Quantity: How to Publish CVEs that Actually Matter

Tags: Red Team Village | Misc

When: Friday, Aug 7, 14:00 - 15:59 PDT

Where: LVCCW Level 1 Hall 1 309 (Red Team Village) Tactic Table 2 - [Map](#)

Description:

This hands-on tactic focuses on making CVE discovery and publication practical, accessible, and repeatable. Instead of treating vulnerability research as an individual or highly specialized skill, this session introduces a structured workflow that attendees can immediately apply.

Attendees will follow a step-by-step approach to:

- Explore a scoped attack surface
- Apply a curated vulnerability pattern checklist
- Identify and validate a potential vulnerability
- Structure the finding in a simplified CVE-style format

All materials are prepared in advance to ensure the activity can be completed within 30–60 minutes and repeated across multiple waves of participants.

This tactic emphasizes doing over theory, helping attendees leave not just with knowledge, but with a clear, reusable method for identifying and documenting vulnerabilities and a better understanding of how CVE publishing can be integrated into team workflows.

SpeakerBio: Natan Morette, Pentest Manager at Thoropass, vulnerability researcher, and cybersecurity instructor for Brazil's national Hackers for Good initiative

Natan Morette is a Penetration Test Manager, vulnerability researcher, and cybersecurity instructor for Brazil's national Hackers for Good initiative, where he mentors students in offensive security across the country. He began his career as a help desk analyst and moved through infrastructure roles before discovering his passion for cybersecurity. Natan has discovered and published multiple CVEs and actively supports students in identifying and disclosing their own—especially in open-source projects with meaningful social impact.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Blacks In Cyber Village - Sunday - 11:00-11:30 PDT

Title: Quantum Computing The Game Changer You Can t Ignore

Tags: Blacks In Cyber Village | Creator Talk/Panel

When: Sunday, Aug 9, 11:00 - 11:30 PDT

Where: LVCCW Level 3 W322-W324 (BIC Village) - [Map](#)

Description:

Quantum computing can feel intimidating, but this session makes it clear, practical, and relevant. Dannielle Eason will break down the basics of quantum computing, explain why it matters now, and show how it may disrupt cybersecurity, healthcare, finance, AI, climate science, and more. Attendees will leave with concrete steps for protecting personal data, preparing organizations for Q-Day, and staying current with NIST, CISA, and NSA guidance. Whether you are technical, non-technical, or simply curious, this welcoming session will help you understand the quantum shift and what to do next.

SpeakerBio: Danielle Eason, Cybersecurity Speaker

Dr. Dannielle Eason is a cybersecurity and governance, risk, and compliance leader with more than 15 years of experience driving enterprise compliance, audit readiness, and federal cybersecurity initiatives. She specializes in building governance frameworks, using data to guide risk decisions, and aligning security strategy with organizational goals. Her work includes leading federal regulatory tracking programs, improving compliance metrics through policy alignment, automating reporting workflows, and strengthening security assessment programs. A frequent speaker at industry conferences including BITECON and GovTechCon, Dr. Eason brings practical expertise in cybersecurity, GRC, and organizational readiness to help audiences understand and prepare for emerging technology risks.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

The Diana Initiative - Friday - 10:20-10:30 PDT

Title: Quantum Village Tour

Tags: The Diana Initiative | Creator Tour

When: Friday, Aug 7, 10:20 - 10:30 PDT

Where: LVCCW Level 1 South Lobby / Atrium - [Map](#)

Description:

Interested in visiting Quantum Village but afraid to go by yourself? The Diana Initiative is hosting tours! Follow a volunteer to Quantum Village and be introduced to the community and activities inside!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Quantum-Ready or Not: What 1,000 Codebases Reveal About Cryptographic Risk

Tags: Crypto & Privacy Village | Creator Talk/Panel

When: Saturday, Aug 8, 16:00 - 16:30 PDT

Where: LVCCW Level 1 Hall 3 1105 (Creator Stage 3) - [Map](#)

Description:

Many people are aware of the quantum threat to cryptography, but how extensive is this issue? We analyzed 1,000* high-profile open-source repositories, including OpenVPN, Curl, and Bitcoin, and found that cryptographic risk is pervasive and hidden. 94% of repositories contain at least one cryptographic issue that would become exploitable in a post-quantum setting*, while 92% contain an issue that is already considered insecure by today's standards*. The median repository contains 185 quantum-relevant weaknesses of moderate severity or higher, nearly double the classical median of 95*, indicating that there is substantial and underrecognized quantum exposure. Notably, thousands of findings are what we call "PQ-invisible;" they appear secure under classical assumptions but would become vulnerable with sufficiently powerful quantum capabilities*, revealing a critical blind spot in current security practices.

These results highlight a gap between real-world cryptography and post-quantum readiness at a time when NIST migration timelines are approaching and Q-Day remains unpredictable. Unlike prior talks that focus on surface-level generalities, this talk is grounded in empirical analysis of source code across a large corpus of highly-used repositories.

We will give a brief overview of the quantum threat, such as current estimates of quantum progress, NIST standardization, and attacks such as Harvest Now, Decrypt Later (HNDL) and Trust Now, Forge Later (TNFL). We will then present our methodology and results, including detailed breakdowns of cryptographic types, algorithms, and security postures across public-key cryptography, symmetric encryption, hashing, password hashing, TLS, and MACs.

Whether you're new to the quantum threat to cryptography or all-too-familiar with it, we hope to provide a clearer understanding of the current state of cryptography and the post-quantum migration.

*Statistics based on an initial sample of 100 repositories; results will be updated as the dataset scales to 1,000.

SpeakerBio: Dr. Zulfikar Ramzan

Dr. Zulfikar Ramzan is Chief Technology and AI Officer at Point Wild, a global leader in AI-powered cybersecurity. He spearheaded the development and launch of Lat61, a highly scalable, extensible AI platform that consolidates data from multiple sources to detect multi-vector attacks, optimize protection across 50+ products and support over 25 million active users. He also leads the Lat61 Threat Intelligence Team, directing research into emerging threats and strengthening Point Wild's Lat61 platform.

Dr. Ramzan has over 20 years of experience in cybersecurity. At Aura, he served as Chief Scientist and Board member, leading the development of AI-driven platforms such as Aura Call Protection, Aura Message Protection, Smart Vault, and the Apollo platform for AI workloads. He has also held senior leadership roles at RSA as Chief Technology Officer and Chief Digital Officer. Earlier in his career, he contributed to Symantec Endpoint Protection and advanced machine learning-powered technologies at Immunit, now part of Cisco. He holds a PhD from MIT and is an inventor on more than 60 patents in cybersecurity and applied cryptography.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

The Diana Initiative - Saturday - 11:50-11:59 PDT

Title: Queercon Community Lounge Tour

Tags: The Diana Initiative | Creator Tour

When: Saturday, Aug 8, 11:50 - 11:59 PDT

Where: LVCCW Level 1 South Lobby / Atrium - [Map](#)

Description:

Interested in visiting Queercon Community Lounge but afraid to go by yourself? The Diana Initiative is hosting tours! Follow a volunteer to Queercon Community Lounge and be introduced to the community and activities inside!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Social Gatherings/Events - Saturday - 16:00-17:59 PDT

Title: Queercon Mixer

Tags: Meetup | Queercon Community

When: Saturday, Aug 8, 16:00 - 17:59 PDT

Where: LVCCW Level 3 W325 (QueerCon Lounge) - [Map](#)

Description:

Come meet the largest social network of LGBTQIA+ and allied hackers at Queercon! Our mixers are designed for you to meet, network, and engage with like-minded people to a backdrop of music, dance, and refreshments.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Social Gatherings/Events - Friday - 16:00-17:59 PDT

Title: Queercon Mixer

Tags: Meetup | Queercon Community

When: Friday, Aug 7, 16:00 - 17:59 PDT

Where: LVCCW Level 3 W325 (QueerCon Lounge) - [Map](#)

Description:

Come meet the largest social network of LGBTQIA+ and allied hackers at Queercon! Our mixers are designed for you to meet, network, and engage with like-minded people to a backdrop of music, dance, and refreshments.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Queercon Community - Friday - 12:00-12:59 PDT

Title: QueerCon Opening Meet and Greet

Tags: Queercon Community | Creator Event/Activity

When: Friday, Aug 7, 12:00 - 12:59 PDT

Where: LVCCW Level 3 W325 (QueerCon Lounge) - [Map](#)

Description:

Join us for the opening of this years queercon lounge

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

The Diana Initiative - Friday - 10:00-01:59 PDT

Title: Quiet Room

Tags: Quiet Room with TDI & MHH | The Diana Initiative | Creator Event/Activity

When: Friday, Aug 7, 10:00 - 01:59 PDT

Where: LVCCW Level 2 W208 (Quiet Room with TDI and MHH) - [Map](#)

Description:

Diana Initiative is excited to offer up a "Quiet Room" again this year. This room is a library vibes environment where people can calm down or recharge before going back out to experience more DEF CON, or even safely have a meltdown, stim, and take time to recenter. In our library area we will have fidget toys, coloring pages and more. This year we are partnering with Mental Health Hackers to make it even better!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

The Diana Initiative - Saturday - 10:00-01:59 PDT

Title: Quiet Room

Tags: Quiet Room with TDI & MHH | The Diana Initiative | Creator Event/Activity

When: Saturday, Aug 8, 10:00 - 01:59 PDT

Where: LVCCW Level 2 W208 (Quiet Room with TDI and MHH) - [Map](#)

Description:

Diana Initiative is excited to offer up a "Quiet Room" again this year. This room is a library vibes environment where people can calm down or recharge before going back out to experience more DEF CON, or even safely have a meltdown, stim, and take time to recenter. In our library area we will have fidget toys, coloring pages and more. This year we are partnering with Mental Health Hackers to make it even better!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

The Diana Initiative - Saturday - 10:00-01:59 PDT

Title: Quiet Room

Tags: Quiet Room with TDI & MHH | The Diana Initiative | Creator Event/Activity

When: Saturday, Aug 8, 10:00 - 01:59 PDT

Where: LVCCW Level 2 W208 (Quiet Room with TDI and MHH) - [Map](#)

Description:

Diana Initiative is excited to offer up a "Quiet Room" again this year. This room is a library vibes environment where people can calm down or recharge before going back out to experience more DEF CON, or even safely have a meltdown, stim, and take time to recenter. In our library area we will have fidget toys, coloring pages and more. This year we are partnering with Mental Health Hackers to make it even better!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

The Diana Initiative - Sunday - 12:17-13:16 PDT

Title: Quiet Room

Tags: Quiet Room with TDI & MHH | The Diana Initiative | Creator Event/Activity

When: Sunday, Aug 2, 12:17 - 13:16 PDT

Where:

Description:

Diana Initiative is excited to offer up a "Quiet Room" again this year. This room is a library vibes environment where people can calm down or recharge before going back out to experience more DEF CON, or even safely have a meltdown, stim, and take time to recenter. In our library area we will have fidget toys, coloring pages and more. This year we are partnering with Mental Health Hackers to make it even better!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Racing PX4: Memory Safety and Timing Vulnerabilities

Tags: Aerospace Village | Creator Talk/Panel

When: Saturday, Aug 8, 14:00 - 14:30 PDT

Where: LVCCW Level 1 Hall 3 1103 (Creator Stage 5) - [Map](#)

Description:

Commercial off-the-shelf autonomous vehicles range from self-driving trucks to military-grade drones. These systems commonly use the PX4 Autopilot flight stack for flight control, navigation, and telemetry. PX4 is a modular stack where logical functions are placed within components. MAVLink is a protocol that facilitates communication between a vehicle and a Ground Control Station. PX4 and its communication facilities are employed in industrial, as well as military environments, where security and correct real-time operation are paramount. This talk will examine how real-time operations and security may be jeopardized by memory corruption and timing-sensitive vulnerabilities in PX4's communication and logging subsystems. Further, this talk will present a novel time-of-check to time-of-use (TOCTOU) race condition in the MAVLink logging subsystem, MavlinkUlog. This results in a Denial-of-Service where vital commands cannot be sent to the vehicle, sequence tracking is thrown off, and telemetry is unreliable. Through this talk, the unique implications of these vulnerabilities upon autonomous systems deployed in safety-critical environments will be discussed.

SpeakerBio: Nefeli Georgilas

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Contests - Sunday - 10:00-10:59 PDT

Title: Radio Frequency Capture the Flag

Tags: Radio Frequency Village | Radio Frequency Capture the Flag | Contest

When: Sunday, Aug 9, 10:00 - 10:59 PDT

Where: LVCCW Level 1 Hall 1 409 (Radio Frequency Village) - [Map](#)

Description:

In this game capture the flag you will be presented with real configurations of real wireless and radio technologies to attack. Practice your skill and learn new ones from Radio Frequency IDentification (RFID) through Software Defined Radio (SDR) and up to Bluetooth and WiFi. There may even be Infrared, if you have the eye for it.

RF Hackers Sanctuary is once again holding the Radio Frequency Capture the Flag (RFCTF) at DEF CON 32. RFHS runs this game to teach security concepts and to give people a safe and legal way to practice attacks against new and old wireless technologies.

We cater to both those who are new to radio communications as well as to those who have been playing for a long time. We are looking for inexperienced players on up to the SIGINT secret squirrels to play our games. The RFCTF can be played with a little knowledge, a pen tester's determination, and \$0 to \$\$\$\$ worth of special equipment. Our virtual RFCTF can be played completely remotely without needing any specialized equipment at all, just using your web browser! The key is to read the clues, determine the goal of each challenge, and have fun learning.

This game doesn't let you sit still either, as there are numerous fox hunts, testing your skill in tracking various signals. If running around the conference looking for WiFi, Bluetooth, or even a Tire Pressure Monitoring System (TPMS) device sounds like fun, we are your source of a higher step count.

There will be clues everywhere, and we will provide periodic updates via discord and twitter. Make sure you pay attention to what's happening at the RFCTF desk, #rfctf on our discord, on Twitter @rf_ctf, @rfhackers, and the interwebz, etc. If you have a question - ASK! We may or may not answer, at our discretion.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Radio Frequency Capture the Flag

Tags: Radio Frequency Village | Radio Frequency Capture the Flag | Contest

When: Friday, Aug 7, 11:00 - 11:59 PDT

Where: Online

Description:

In this game capture the flag you will be presented with real configurations of real wireless and radio technologies to attack. Practice your skill and learn new ones from Radio Frequency IDentification (RFID) through Software Defined Radio (SDR) and up to Bluetooth and WiFi. There may even be Infrared, if you have the eye for it.

RF Hackers Sanctuary is once again holding the Radio Frequency Capture the Flag (RFCTF) at DEF CON 32. RFHS runs this game to teach security concepts and to give people a safe and legal way to practice attacks against new and old wireless technologies.

We cater to both those who are new to radio communications as well as to those who have been playing for a long time. We are looking for inexperienced players on up to the SIGINT secret squirrels to play our games. The RFCTF can be played with a little knowledge, a pen tester's determination, and \$0 to \$\$\$\$ worth of special equipment. Our virtual RFCTF can be played completely remotely without needing any specialized equipment at all, just using your web browser! The key is to read the clues, determine the goal of each challenge, and have fun learning.

This game doesn't let you sit still either, as there are numerous fox hunts, testing your skill in tracking various signals. If running around the conference looking for WiFi, Bluetooth, or even a Tire Pressure Monitoring System (TPMS) device sounds like fun, we are your source of a higher step count.

There will be clues everywhere, and we will provide periodic updates via discord and twitter. Make sure you pay attention to what's happening at the RFCTF desk, #rfctf on our discord, on Twitter @rf_ctf, @rfhackers, and the interwebz, etc. If you have a question - ASK! We may or may not answer, at our discretion.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Contests - Saturday - 10:00-17:59 PDT

Title: Radio Frequency Capture the Flag

Tags: Radio Frequency Village | Radio Frequency Capture the Flag | Contest

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 409 (Radio Frequency Village) - [Map](#)

Description:

In this game capture the flag you will be presented with real configurations of real wireless and radio technologies to attack. Practice your skill and learn new ones from Radio Frequency IDentification (RFID) through Software Defined Radio (SDR) and up to Bluetooth and WiFi. There may even be Infrared, if you have the eye for it.

RF Hackers Sanctuary is once again holding the Radio Frequency Capture the Flag (RFCTF) at DEF CON 32. RFHS runs this game to teach security concepts and to give people a safe and legal way to practice attacks against new and old wireless technologies.

We cater to both those who are new to radio communications as well as to those who have been playing for a long time. We are looking for inexperienced players on up to the SIGINT secret squirrels to play our games. The RFCTF can be played with a little knowledge, a pen tester's determination, and \$0 to \$\$\$\$ worth of special equipment. Our virtual RFCTF can be played completely remotely without needing any specialized equipment at all, just using your web browser! The key is to read the clues, determine the goal of each challenge, and have fun learning.

This game doesn't let you sit still either, as there are numerous fox hunts, testing your skill in tracking various signals. If running around the conference looking for WiFi, Bluetooth, or even a Tire Pressure Monitoring System (TPMS) device sounds like fun, we are your source of a higher step count.

There will be clues everywhere, and we will provide periodic updates via discord and twitter. Make sure you pay attention to what's happening at the RFCTF desk, #rfctf on our discord, on Twitter @rf_ctf, @rfhackers, and the interwebz, etc. If you have a question - ASK! We may or may not answer, at our discretion.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Radio Frequency Capture the Flag

Tags: Radio Frequency Village | Radio Frequency Capture the Flag | Contest

When: Friday, Aug 7, 11:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 409 (Radio Frequency Village) - [Map](#)

Description:

In this game capture the flag you will be presented with real configurations of real wireless and radio technologies to attack. Practice your skill and learn new ones from Radio Frequency IDentification (RFID) through Software Defined Radio (SDR) and up to Bluetooth and WiFi. There may even be Infrared, if you have the eye for it.

RF Hackers Sanctuary is once again holding the Radio Frequency Capture the Flag (RFCTF) at DEF CON 32. RFHS runs this game to teach security concepts and to give people a safe and legal way to practice attacks against new and old wireless technologies.

We cater to both those who are new to radio communications as well as to those who have been playing for a long time. We are looking for inexperienced players on up to the SIGINT secret squirrels to play our games. The RFCTF can be played with a little knowledge, a pen tester's determination, and \$0 to \$\$\$\$ worth of special equipment. Our virtual RFCTF can be played completely remotely without needing any specialized equipment at all, just using your web browser! The key is to read the clues, determine the goal of each challenge, and have fun learning.

This game doesn't let you sit still either, as there are numerous fox hunts, testing your skill in tracking various signals. If running around the conference looking for WiFi, Bluetooth, or even a Tire Pressure Monitoring System (TPMS) device sounds like fun, we are your source of a higher step count.

There will be clues everywhere, and we will provide periodic updates via discord and twitter. Make sure you pay attention to what's happening at the RFCTF desk, #rfctf on our discord, on Twitter @rf_ctf, @rfhackers, and the interwebz, etc. If you have a question - ASK! We may or may not answer, at our discretion.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Radio Frequency Village - Saturday - 10:00-17:59 PDT

Title: Radio Frequency Village Events

Tags: Radio Frequency Village | Creator Event/Activity

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 409 (Radio Frequency Village) - [Map](#)

Description:

In addition to the CTF and talks, which are elsewhere on the schedule, the RF Village is also a place to hang out and chat with like minded folks who share your interests.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Radio Frequency Village - Friday - 10:00-17:59 PDT

Title: Radio Frequency Village Events

Tags: Radio Frequency Village | Creator Event/Activity

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 409 (Radio Frequency Village) - [Map](#)

Description:

In addition to the CTF and talks, which are elsewhere on the schedule, the RF Village is also a place to hang out and chat with like minded folks who share your interests.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Radio Frequency Village - Sunday - 10:00-13:59 PDT

Title: Radio Frequency Village Events

Tags: Radio Frequency Village | Creator Event/Activity

When: Sunday, Aug 9, 10:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 1 409 (Radio Frequency Village) - [Map](#)

Description:

In addition to the CTF and talks, which are elsewhere on the schedule, the RF Village is also a place to hang out and chat with like minded folks who share your interests.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

The Diana Initiative - Saturday - 11:20-11:30 PDT

Title: Radio Frequency Village Tour

Tags: The Diana Initiative | Creator Tour

When: Saturday, Aug 8, 11:20 - 11:30 PDT

Where: LVCCW Level 1 South Lobby / Atrium - [Map](#)

Description:

Interested in visiting Radio Frequency Village but afraid to go by yourself? The Diana Initiative is hosting tours! Follow a volunteer to Radio Frequency Village and be introduced to the community and activities inside!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Rage Against the Sandbox: Bypassing Apple's iOS Security to Run Unsigned Code via SSH

Tags: DEF CON Official Talk | Demo | Tool

When: Saturday, Aug 8, 12:00 - 12:59 PDT

Where: LVCCW Level 1 Hall 3 1006 (Main Track 1) - [Map](#)

Description:

Apple's Sandbox and code signing have made traditional security research impractical on iPhones - researchers must use full-system emulation or hunt for increasingly rare jailbreak exploits. The Sandbox blocks `fork()`, which shells need for job control. Code signing prevents unsigned code execution.

We present techniques that bypass both restrictions without exploiting vulnerabilities. Using only standard APIs, we built a system that runs SSH servers and interactive shells on iPhones with full `fork()` support and unsigned code execution.

We'll dive deep into the technical implementation: userspace memory management, thread-based process virtualization, stack frame manipulation, and selective CPU emulation. Then we'll demonstrate the real impact: running an unsigned public exploit directly on an iPhone through SSH - no jailbreak, no signing, no problem.

Full paper I wrote about the talk (have not published it in public domains yet, waiting for the conference first as a reveal!)

"Rage Against the Sandbox: Bypassing Apple's iOS Security to Run Unsigned Code via SSH", Y.H. Hirschenbein Sadde, 2026 <https://drive.google.com/file/d/1ZyIvQa3kjiLvCmNhdY-fmSAbhRA5gLPx/view>

SpeakerBio: Yuval Hanoch Hirschenbein Sadde

Yuval is a security researcher. His main focuses are Android and iOS security - specifically in low-level system code and kernel modules. His work centers around researching the bootstrap process of operating systems, and analyzing popular low-level code flows within the platform frameworks and their third-party dependencies.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

IoT Village - Sunday - 10:00-13:59 PDT

Title: Raiders of the Lost Firmware: A Hands-On Workshop in IoT Firmware Archaeology

Tags: IoT Village | Creator Workshop

When: Sunday, Aug 9, 10:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 1 215 (IoT Village) - [Map](#)

Description:

Encrypted IoT firmware doesn't have to be a dead end. In this hands-on workshop, we'll reconstruct a real vendor's firmware decryption pipeline without ever touching the hardware...



[Return to Index](#) - Add to Google - ics [Calendar](#) file

IoT Village - Friday - 10:00-17:59 PDT

Title: Raiders of the Lost Firmware: A Hands-On Workshop in IoT Firmware Archaeology

Tags: IoT Village | Creator Workshop

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 215 (IoT Village) - [Map](#)

Description:

Encrypted IoT firmware doesn't have to be a dead end. In this hands-on workshop, we'll reconstruct a real vendor's firmware decryption pipeline without ever touching the hardware...



[Return to Index](#) - Add to Google - ics [Calendar](#) file

IoT Village - Saturday - 10:00-17:59 PDT

Title: Raiders of the Lost Firmware: A Hands-On Workshop in IoT Firmware Archaeology

Tags: IoT Village | Creator Workshop

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 215 (IoT Village) - [Map](#)

Description:

Encrypted IoT firmware doesn't have to be a dead end. In this hands-on workshop, we'll reconstruct a real vendor's firmware decryption pipeline without ever touching the hardware...



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Raiders of the Lost Firmware: A Hands-On Workshop in IoT Firmware Archaeology

Tags: IoT Village | Creator Talk/Panel

When: Saturday, Aug 8, 12:30 - 13:30 PDT

Where: LVCCW Level 1 Hall 3 1105 (Creator Stage 3) - [Map](#)

Description:

Modern IoT firmware often appears protected behind proprietary encryption, stopping analysis before it starts. However, in many cases the fastest path forward is not to break the cryptography, but it is to reuse the vendor's own implementation via targeted function emulation. In this hands-on workshop, attendees will learn a methodology we call firmware archaeology: a practical method for reconstructing the proprietary firmware decryption scheme by correlating artifacts left behind across firmware archives, public repositories and developer ecosystems. Attendees will analyze the real-world ecosystem of a commercial IP camera vendor, using the firmware archaeology methodology. First, they will identify historical artifacts and ecosystem components from publicly available sources. Next, they will recover from binaries the cryptographic routines that are responsible for decrypting the firmware images. They will then reuse and emulate these functions in a controlled environment to recover the decrypted firmware image that was initially secured by the proprietary encryption scheme. With this access, participants will move beyond decryption to explore hidden functionalities of the target device and map the broader attack surface of the platform that was previously inaccessible. The workshop is designed as a practical methodology session rather than a one-off trick or a showcase of vulnerabilities. All exercises are hands-on and based on real research, with pre-packaged material and tooling provided. Attendees will leave with a practical and repeatable methodology for analyzing modern IoT platforms, including techniques to reconstruct firmware decryption pipelines and bypass analysis barriers without reimplementing vendor cryptography from scratch.

Speakers: Simone Bossi, Luca Borzacchiello

SpeakerBio: Simone Bossi

Simone takes apart embedded systems and firmware for a living, but it took a while to get there. He started doing vulnerability research in 2015 on web, mobile, network, and the occasional cryptography rabbit hole, including a stint as a cryptanalyst at STMicroelectronics working on IoT communications security. Around 2020 he moved fully into IoT and OT, where bugs live in proprietary protocols, firmware nobody was meant to read, and hardware that was built to last, not to be secured.

He now leads the vulnerability research team at Nozomi Networks Labs, where they find 0-days in industrial and IoT devices, and quickly learned that the most interesting features are the ones you don't find in the user manual. Along the way: academic research on weaknesses in Linux's cryptsetup and PBKDF2 that made it into the security literature, open-source offensive tooling, and RE sessions old enough to have developed opinions.

SpeakerBio: Luca Borzacchiello, Nozomi Networks

Luca Borzacchiello is a Security Researcher with deep expertise in Symbolic Execution, Reverse Engineering, and Fuzzing. He currently works at Nozomi Networks, where he focuses on cutting-edge security research. Before joining Nozomi, Luca served as a Red Team Engineer for the Italian Government, where he contributed to national cybersecurity initiatives. He also worked as researcher on the Red Team at TIM S.p.A., one of Italy's leading telecommunications companies. Luca holds a Ph.D. in Program Analysis from Sapienza University of Rome. Outside of work, he is an active participant in Capture The Flag (CTF) competitions, where he enjoys applying his reverse engineering skills in high-stakes challenges.

Title: Raitlin's Challenge

Tags: Raitlin's Challenge | Contest

When: Wednesday, Aug 5, 22:00 - 22:59 PDT

Where: Online

Description:

Test your mental abilities with Raitlin's Challenge, the Illuminati Party®'s sophisticated collection of abstract visual puzzles, presented annually at DEF CON for over a decade. This intellectually demanding competition pushes participants to their limits through exceedingly complex challenges that require mastery of diverse knowledge domains.

The challenge begins with an initial invitation puzzle that serves as a gateway to the main experience. Once solved, competitors continue to a carefully curated series of abstract visual puzzles presented in an artistically refined format on the dedicated website. Each puzzle solved yields a verification string for validation and progress tracking.

What sets Raitlin's Challenge apart is its comprehensive scope, drawing upon principles from mathematics, science, engineering, technology, cryptography, protocols, algorithms, biology, chemistry, programming, and ancient history. While technical expertise, particularly in hacking, proves advantageous, the true challenge lies in applying abstract thinking across multiple disciplines.

The journey to completion varies significantly among participants, spanning anywhere from days to years. Unlike many competitive events, Raitlin's Challenge remains perpetually available after DEF CON concludes, allowing determined solvers to pursue solutions at their own pace. Those who ultimately succeed earn recognition on the prestigious ledger of completions, joining an elite group of problem-solvers who have demonstrated exceptional intellectual versatility and persistence in unraveling the secrets of the Illuminati Party®.

Participant Prerequisites

Access to a web browser and Internet connection.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: RASM: A State Machine Methodology for RF Security Assessment

Tags: Radio Frequency Village | Creator Talk/Panel

When: Saturday, Aug 8, 14:00 - 14:55 PDT

Where: LVCCW Level 1 Hall 1 409 (Radio Frequency Village) - [Map](#)

Description:

RF security assessment is fundamentally different from traditional application or network testing. Signals are invisible, environmental conditions influence behavior, protocols are often undocumented, and even small physical changes can alter outcomes in unexpected ways. Unlike conventional targets, RF systems rarely expose stable interfaces, useful diagnostics, or predictable attack paths. This talk introduces RASM (RF Attack State Machine), a methodology and state-aware research tool designed specifically for offensive RF investigations. Rather than treating assessment as a linear checklist, RASM models RF hacking as movement through interconnected operational states — from target understanding and signal discovery to demodulation, protocol analysis, manipulation, and validated exploitation. RASM operationalizes this methodology by helping researchers navigate RF investigations contextually. Information gathered during earlier stages influences recommendations, tooling choices, investigative paths, and subsequent transitions throughout the assessment process. Instead of attempting to automate RF analysis itself, the framework focuses on guiding researchers through the uncertainty and iterative decision-making that characterize real-world wireless security work. The session includes a live walkthrough of the RASM tool, demonstrating how researchers move through assessment states against a real RF target. It is intended for security researchers, SDR practitioners, hardware hackers, and anyone exploring offensive RF methodology and wireless security research workflows.

SpeakerBio: Smriti Gaba

No BIO available

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Contests - Sunday - 10:00-11:59 PDT

Title: Reali7y Overrun - Contest running

Tags: Reali7y Overrun | Contest

When: Sunday, Aug 9, 10:00 - 11:59 PDT

Where: LVCCW Level 1 Hall 1 308 (Reali7y Overrun) - [Map](#)

Description:

Enter a near future dystopia where AI is threatening to take over the world through misinformation campaigns and leveraged takeover of automation technology. Join us for online and real world challenges, including an AI racecar challenge.

Friday and Saturday AI "deepracer" style car races at the event booth racetrack: * Noon * 2pm * 4pm

Sunday: Final scoring

All race times may have one or more race events. All race events are up to 3 simultaneous racers.

** YOU MUST COMPLETE IN-GAME CONTENT TO QUALIFY TO RACE. **

** Good luck! **

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Contests - Saturday - 10:00-17:59 PDT

Title: Reali7y Overrun - Contest running

Tags: Reali7y Overrun | Contest

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 308 (Reali7y Overrun) - [Map](#)

Description:

Enter a near future dystopia where AI is threatening to take over the world through misinformation campaigns and leveraged takeover of automation technology. Join us for online and real world challenges, including an AI racecar challenge.

Friday and Saturday AI "deepracer" style car races at the event booth racetrack: * Noon * 2pm * 4pm

Sunday: Final scoring

All race times may have one or more race events. All race events are up to 3 simultaneous racers.

** YOU MUST COMPLETE IN-GAME CONTENT TO QUALIFY TO RACE. **

** Good luck! **

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Contests - Friday - 10:00-17:59 PDT

Title: Reali7y Overrun - Contest running

Tags: Reali7y Overrun | Contest

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 308 (Reali7y Overrun) - [Map](#)

Description:

Enter a near future dystopia where AI is threatening to take over the world through misinformation campaigns and leveraged takeover of automation technology. Join us for online and real world challenges, including an AI racecar challenge.

Friday and Saturday AI "deepracer" style car races at the event booth racetrack: * Noon * 2pm * 4pm

Sunday: Final scoring

All race times may have one or more race events. All race events are up to 3 simultaneous racers.

** YOU MUST COMPLETE IN-GAME CONTENT TO QUALIFY TO RACE. **

** Good luck! **

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Rebuilding Code Security with Signal, Speed and AI

Tags: AppSec Village | Creator Event/Activity || All Audiences

When: Friday, Aug 7, 16:30 - 17:30 PDT

Where: LVCCW Level 1 Hall 2 604 (Appsec Village) Arsenal - [Map](#)

Description:

Modern AppSec tooling is fragmented: one scanner for secrets, another for dependencies, another for SAST, another for containers, another for SBOMs, and then a separate workflow for triage. Broly is an open source Go scanner built to collapse that workflow into one fast App and finding model.

This Arsenal session walks through Broly's current design: Titus-backed secrets scanning, osv-scalibr + OSV.dev dependency analysis, Together AI powered SAST, container image scanning, license policy checks, SBOM output with baselines, incremental scans, SARIF/JSON/table output, and built in AI triage with optionality. The demo will show Broly scanning a vulnerable repo, producing actionable findings, filtering noise and fitting into a PR workflow.

The session is also a candid engineering case study on what broke, what was rebuilt, where & how AI helped, where deterministic engines still lead, and why security tools need to be attacked with the same rigor as the code they judge.

Speakers:Derek C.,Shasheen Bandodkar

SpeakerBio: Derek C.

Derek is the Head of Security at Together.ai and the former Head of Infrastructure Security at Cloudflare. He has over 20 years of experience in designing security frameworks at scale. His main focus is on research and development within the fields of encryption and infrastructure security.

He earned a masters in cybersecurity from Purdue University and now owns more than 60 global patents related to cryptography, key management, and distributed ledger technology.

SpeakerBio: Shasheen Bandodkar

Shasheen Bandodkar is a security engineer passionate about safeguarding technology and innovation. With deep cybersecurity expertise, he frequently shares insights on his blog and is known for turning rants into revelations.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Recon Village - Sunday - 12:00-12:30 PDT

Title: Recon on Trial: The OSINT Operator's Legal Playbook

Tags: Recon Village | Creator Talk/Panel

When: Sunday, Aug 9, 12:00 - 12:30 PDT

Where: LVCCW Level 1 Hall 3 1103 (Creator Stage 5) - [Map](#)

Description:

You scrape a public site. You enumerate subdomains. You grep GitHub for secrets. You curl a misconfigured API. Each one touches a statute. Some have been to the Supreme Court. Most operators don't know which is which — until the preservation letter arrives. A federal-court-qualified expert witness (U.S. v. Sullivan) walks through five live OSINT techniques with real-time legal annotation. Zero lawyer-speak. GitHub release included.

SpeakerBio: David Cass, Expert Consultant · Head of FinTech Practice

David Cass occupies a vantage point few cybersecurity and financial-technology experts can claim: he has sat on every side of the table. He recently served as a lead regulator at the Federal Reserve Bank of New York, where he was a member of the Large Institution Supervising Coordinating Committee (LISCC) overseeing the systemically important institutions whose security and risk practices he had spent two decades building from the inside. As Head of the FinTech Practice at Law & Forensics and a member of the firm's Cyber Security and Forensics Practice, he brings that supervisory perspective to bear as a testifying expert and consultant — most recently as a cybersecurity expert witness on a significant cyber-attack against a regional credit union that compromised member data and disrupted services.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

The Diana Initiative - Saturday - 13:00-13:10 PDT

Title: Recon Village Tour

Tags: The Diana Initiative | Creator Tour

When: Saturday, Aug 8, 13:00 - 13:10 PDT

Where: LVCCW Level 1 South Lobby / Atrium - [Map](#)

Description:

Interested in visiting Recon Village but afraid to go by yourself? The Diana Initiative is hosting tours! Follow a volunteer to Recon Village and be introduced to the community and activities inside!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Red Robin: Don't Hack For Me, Hack With Me

Tags: La Villa Community | Creator Talk/Panel

When: Sunday, Aug 9, 12:00 - 12:59 PDT

Where: LVCCW Level 1 Hall 4 1416 (La Villa Community) Main Stage - [Map](#)

Description:

Desde 2025, y especialmente con la llegada de modelos de IA cada vez más capaces, el panorama de la ciberseguridad ha visto una explosión de herramientas de hacking impulsadas por IA. Prometen explotación automatizada. El objetivo de muchas de estas herramientas es ser 100% autónomas, con el hacker fuera del loop. Pero esto es seguridad: sistemas en producción, datos sensibles. Una operación real no mide solo la tecnología, también a las personas y los procedimientos, cómo detectan y cómo responden. Sin contexto y sin alguien que responda por cada decisión, automatizar no alcanza.

Esta charla presenta Red Robin, un compañero de IA por línea de comandos hecho específicamente para red teamers. Red Robin se integra con tu framework de Command-and-Control (C2), observa la actividad de tus beacons a medida que ocurre, y te da guía contextual en tiempo real anclada a tus objetivos operativos. Nunca actúa por su cuenta. No hackea por vos. Piensa con vos.

Esta charla cubre el panorama actual de hacking humano-vs-IA, la filosofía detrás del modelo de compañero, una inmersión técnica en la arquitectura de Red Robin, una demostración en vivo de Red Robin construyendo situational awareness dentro de una sesión de C2 activa, y una discusión a futuro sobre dónde debería encajar la asistencia de IA en el futuro de la seguridad ofensiva.

Speakers: Juan Sequeira Piedra, Jose Urena

SpeakerBio: Juan Sequeira Piedra, Red Team Operator - Equifax

Juan Sequeira es un operador de red team que ejecuta full-scope adversary emulation en entornos empresariales. Llegó a “offensive security” desde el lado defensivo tras dos años en un SOC, y hoy trabaja en desarrollo de malware, infraestructura y automatización de red team, e investigación de seguridad. Ha representado a Team Latin America en el International Cybersecurity Challenge 2026 en Gold Coast, Australia, y a Team Costa Rica en el European Cybersecurity Challenge (Turín 2024, Varsovia 2025) y en el Latin America Cybersecurity Challenge 2025 (Medellín).

SpeakerBio: Jose Urena, Equifax - Red Team Operator

Jose Urena es un Red Team Lead con experiencia y más de nueve años trabajando en la industria de la ciberseguridad, especializado en investigación de vulnerabilidades, desarrollo seguro y operaciones ofensivas avanzadas. Su trayectoria abarca roles críticos en auditoría de seguridad, desarrollo de herramientas y simulación de adversarios en entornos empresariales complejos. Jose es un contribuidor activo de la comunidad de seguridad y ha presentado anteriormente sobre Red Teaming, aplicación práctica de IA y operaciones de ataque modernas en el Ministerio de Ciencia y Tecnología (MICITT) de Costa Rica, así como en Kennesaw State University en Georgia.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Red Team Village - Friday - 10:00-11:59 PDT

Title: Red Team Express

Tags: Red Team Village | Misc

When: Friday, Aug 7, 10:00 - 11:59 PDT

Where: LVCCW Level 1 Hall 1 309 (Red Team Village) Tactic Table 2 - [Map](#)

Description:

We have a train that needs to keep going. The defender needs to keep the train going. The attacker needs to stop the train. Who will win?

This tactic would explore OT protocols (such as modbus) to control a Lego train. Participants can watch, or participate as either an attacker or defender. Their goals being to either stop the train or keep it on track.

SpeakerBio: Cody Spooner

This will change

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

The Diana Initiative - Saturday - 13:30-13:40 PDT

Title: Red Team Village Tour

Tags: The Diana Initiative | Creator Tour

When: Saturday, Aug 8, 13:30 - 13:40 PDT

Where: LVCCW Level 1 South Lobby / Atrium - [Map](#)

Description:

Interested in visiting Red Team Village but afraid to go by yourself? The Diana Initiative is hosting tours! Follow a volunteer to Red Team Village and be introduced to the community and activities inside!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Red Team Village - Saturday - 12:00-13:59 PDT

Title: Red Teaming Kubernetes: From App-Level CVEs to Full Cluster Takeover

Tags: Red Team Village | Misc

When: Saturday, Aug 8, 12:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 1 309 (Red Team Village) Tactic Table 4 - [Map](#)

Description:

Kubernetes is the de facto operating system of the cloud, and more and more organizations are running their workloads on Kubernetes. While Kubernetes offers many benefits, it also introduces new security risks, such as cluster misconfiguration, leaked credentials, cryptojacking, container escapes, and vulnerable clusters.

In this workshop, attendees will learn how to attack Kubernetes clusters by simulating a real-world adversary exploiting one of the most recent vulnerabilities in the ecosystem: IngressNightmare (CVE-2025-1974). Participants will practice exfiltrating service account tokens and credentials, performing lateral movement, escalating privileges by targeting common applications deployed in Kubernetes environments, and ultimately compromising the entire cluster.

SpeakerBio: Lenin Alevski, Security Engineer at Google

Lenin Alevski is a Full Stack Engineer and generalist with a lot of passion for Information Security. Currently working as a Security Engineer at Google. Lenin specializes in building and maintaining Distributed Systems, Application Security and Cloud Security in general. Lenin loves to play CTFs, contributing to open-source and writing about security and privacy on his personal blog <https://www.alevsk.com>.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: RedMatter: Let AI Write Your Cross-Platform Mobile Exploits

Tags: Mobile Hacking Community | Creator Talk/Panel

When: Saturday, Aug 8, 10:00 - 10:59 PDT

Where: LVCCW Level 1 Hall 4 1422 (Mobile Hacking Community) - [Map](#)

Description:

Live demo:

Redmatter kills the rewrite. You describe the attack you want in plain language like, bypass the pinning, dump the keychain, defeat the root check, and an AI layer generates the platform-specific Frida instrumentation for both the iOS and Android build of the same app. The harness orchestrates the run, adapts when the app fights back (new detection logic, obfuscation, a symbol that moved), and captures the evidence. You stay in the loop; the AI eats the tedious per-platform translation that used to eat your engagement.

Key takeaways: - Describe an attack in plain English on stage, watch the AI emit working iOS and Android modules, and fire them live on both builds side by side. - Throw a hardened target at it, like anti-Frida, pinning, root detection stacked, and let the harness adapt in real time.

SpeakerBio: Subho Halder, Founder at MatterSec Labs

Subho Halder is the founder of MatterSec Labs, an AI security company, and a mobile security researcher with over a decade in offensive AppSec. He is the author of the Android Framework for Exploitation (AFE), one of the early open-source toolkits for Android app exploitation, which he has used to train operators on the BlackHat US instructor circuit. More recently he released KnoxSpy, a Frida-based instrumentation tool for intercepting MDM-protected traffic, at BlackHat Europe Arsenal 2025.

Before MatterSec, he co-founded Appknox, a mobile application security platform, and ran it for over ten years. His work sits at the intersection of iOS/Android binary analysis, runtime instrumentation, and AI-driven offensive tooling. He is now building Redmatter, the open-source harness debuting in this talk.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Red Team Village - Friday - 16:00-17:59 PDT

Title: redStack: Boot-To-Breach Red Team Platform

Tags: Red Team Village | Misc

When: Friday, Aug 7, 16:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 309 (Red Team Village) Tactic Table 2 - [Map](#)

Description:

Prerequisites: complete these before the session, published in advance at <https://github.com/BaddKharma/redStack-defcon34> (AWS account, AWS CLI, Terraform, and an OpenVPN client). Setup happens ahead of time so it does not eat into the session.

A two-hour hands-on workshop where attendees stand up a full red team operator stack (<https://github.com/BaddKharma/redStack>) and run it against a live cyber range. Each attendee gets their own instanced range over an OpenVPN tunnel, so no public DNS or exposed infrastructure is required. You leave with a working lab to build your own tradecraft and OPSEC on.

Scope: an intermediate session. It assumes some familiarity with pentest or red team topics, comfort on a Linux command line, and a working understanding of what a C2 framework does. Deep AWS or Terraform experience is not required, but you must arrive with the prerequisites completed.

What you build and run: a full operator stack on AWS from a single Terraform apply. Three C2 frameworks (Mythic, Sliver, and Adaptix), an Apache redirector that gates traffic on a header token and CDN-style URI routing with a decoy page for anything that fails, a Guacamole portal for browser-based access to every host, and Kali and Windows operator boxes. You stand each C2 up behind the redirector, then drive a boot-to-breach chain against the live range to SYSTEM.

What it is not: an Active Directory exploitation course. The initial domain compromise is white-carded, so attendees start from a provided Administrator hash and spend the time standing up and driving the platform rather than working the AD chain. Web exploitation, custom payload development, and AV or EDR evasion are out of scope.

Target: a per-user-instanced Hack Smarter Labs range (a Windows Server 2022 domain controller) reached over an OpenVPN tunnel, so no two attendees touch the same box. Everything runs in your own throwaway AWS account and is destroyed at the end. redStack is open source, so you keep a lab you can redeploy on your own after the workshop.

Agenda: 10min Intro and setup check. 30min Deploy the stack from one Terraform apply, narrated live. The tunnel comes up, and the range becomes reachable. 5min Break 30min Stand up the three C2 backends (Sliver, Mythic, Adaptix) behind the redirector, test a beacon from each. 5min Break 25min Attack the live range together: Sliver beacon for initial access, Mythic and Adaptix staged through it, SYSTEM on the DC. 10min Q&A and teardown (terraform destroy!)

Speakers: Michael Kim, Michael Ortiz

SpeakerBio: Michael Kim

Michael Kim's journey into cybersecurity is a story of resilience and reinvention. Having lived in seven countries, he faced relentless bullying, racism, and isolation - challenges that once pushed him to the brink. After pursuing paths in veterinary medicine, pharmacy, law, and biology, and graduating with a zoology degree, he shifted careers entirely during the pandemic, leaving behind a career as a DJ and music producer to chase a new purpose in cybersecurity. Through persistence and countless failures, he rose from a boot camp graduate to a Senior Consultant in Offensive Security at Palo Alto Networks Unit 42, leading red team operations, adversary simulations, and penetration tests for global clients. His multicultural background and lived experiences shape his unique approach to hacking and problem-solving, and his story proves that adversity can be transformed into strength - and that anyone, no matter their past, can build a powerful career in cybersecurity.

SpeakerBio: Michael Ortiz

Michael Ortiz is a Red Team Engineer and SME on the U.S. Department of State's Red Cell, running adversary emulation across State enterprise and partner networks. His focus spans offensive tradecraft, evasion engineering against modern EDR's, and the cybersecurity engineering behind durable red team infrastructure. He's the founder of devZero Security, an SDVOSB offering offensive security and security engineering services to federal and commercial clients, and the developer of redStack, an open source AWS and Terraform project that stands up a full red team operations stack on demand. A Marine Corps veteran, Mike holds OSEP, OSCP, CRT0, and CRTL, among other certifications.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: redStack: Boot-to-Breach Red Team Platform

Tags: Noob Community | Creator Workshop

When: Saturday, Aug 8, 13:00 - 14:50 PDT

Where: LVCCW Level 1 Hall 4 1417 (Noob Community) - [Map](#)

Description:

This 2-hour, hands-on training is built around redStack - the open-source AWS project Mike developed to stand up a red team environment on demand. One Terraform command deploys an entire operator stack: three C2 frameworks (Mythic, Sliver, and Havoc), Kali and Windows hosts, a redirector, and a Guacamole portal.

SpeakerBio: Michael Ortiz

Michael Ortiz is a Red Team Engineer and SME on the U.S. Department of State's Red Cell, running adversary emulation across State enterprise and partner networks. His focus spans offensive tradecraft, evasion engineering against modern EDR's, and the cybersecurity engineering behind durable red team infrastructure. He's the founder of devZero Security, an SDVOSB offering offensive security and security engineering services to federal and commercial clients, and the developer of redStack, an open source AWS and Terraform project that stands up a full red team operations stack on demand. A Marine Corps veteran, Mike holds OSEP, OSCP, CRTO, and CRTL, among other certifications.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Reflections on Disregarding Trust (Weaponizing CDP and MHTML for Header-Agnostic Session Hijacking)

Tags: DEF CON Official Talk | Demo | Tool | Exploit

When: Friday, Aug 7, 10:30 - 11:30 PDT

Where: LVCCW Level 1 Hall 3 904 (Main Track 4) - [Map](#)

Description:

Adversary-in-the-Middle (AitM) phishing has become the de facto standard for bypassing legacy Multi-Factor Authentication (MFA). However, modern AitM frameworks rely on complex, fragile regex rules to rewrite HTTP streams on the fly. When target applications implement strict client-side security headers like Subresource Integrity (SRI) and Content Security Policy (CSP), traditional proxies break, alerting defenders.

This presentation introduces a novel "Browser-in-the-Middle" architecture. By weaponizing the Chrome DevTools Protocol (CDP), this custom-built Go toolkit renders the target application server-side, allows legitimate scripts to execute, and captures the resulting DOM as an MHTML snapshot. I will demonstrate how converting external assets into Base64 Data URIs and serving a self-contained, live DOM neutralizes SRI and CSP organically without triggering browser security violations. Finally, the talk will detail a Just-In-Time (JIT) JavaScript shim that hooks API calls to silently harvest post-MFA tokens from major IdPs including Okta, Microsoft, Google, and Shibboleth effectively trapping the user in a perfectly mirrored, attacker-controlled environment.

SpeakerBio: Gregory "lumberhack" Disney-Leugers, Independent Researcher

Gregory Disney-Leugers (lumberhack) is a Independent Researcher specializing in adversary simulation, modern web authentication bypasses, and identity-based attacks. With over a decade of experience in red teaming and penetration testing since 2013, they have previously served as a Technical Lead at major technology and identity providers, including Juniper Networks and Okta.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Relocatable Nix Binaries

Tags: Nix Vegas Community | Creator Talk/Panel

When: Friday, Aug 7, 14:00 - 14:30 PDT

Where: LVCCW Level 1 Hall 4 1310 (Nix Vegas Community) - [Map](#)

Description:

Nix's guarantee of reproducibility hinges on a simple mechanism: absolute, immutable store paths (i.e. `/nix/store`). While this rigidity guarantees that binaries always find their exact dependencies, it introduces a massive constraint: it binds the entire ecosystem to a single, global directory. If you want to run a Nix binary on a target system where you don't have root access to create `/nix`, or where you cannot run an unprivileged user namespace, you are forced to rebuild the world. To achieve true portability and friction-free deployment across arbitrary infrastructure, Nix binaries must become fully relocatable. What does that mean? Why is it hard? Who cares (psst me!)? We will discuss what a fully relocatable Nix ecosystem could look like, and how solving this constraint could allow Nix to be run more easily on more restrictive environments..

SpeakerBio: Farid Zakaria

I'm a software engineer, father and wishful amateur surfer. If you've come seeking my political views, you've found the wrong. You can find my writings on Nix, build systems and software engineering in general at <https://fzakaria.com>



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Requiem for the Decommissioned: When Dead Hosts Bite Back

Tags: Red Team Village | Misc

When: Saturday, Aug 8, 15:00 - 15:59 PDT

Where: LVCCW Level 1 Hall 1 309 (Red Team Village) Workshop Stage 1 - [Map](#)

Description:

Workshop: Requiem for the Decommissioned: When Dead Hosts Bite Back

Every organization has a graveyard - hosts that were decommissioned after a migration, abandoned when a project died, or simply dropped from inventory after a reorg. They're off the asset list, out of the patch cycle, and completely out of mind. They're also still on the network.

This talk breaks down how forgotten and abandoned hosts consistently become the softest entry points during red team engagements - built from real engagement experience across large-scope assessments and bug bounty programs. We'll cover why they keep appearing, why they survive undetected, and how to systematically hunt for them using low-noise reconnaissance techniques.

Attendees will leave with a practical methodology they can apply on their next engagement.

Tactic: Hunting the Decommissioned: Hands-on Forgotten Host Discovery In this hands-on session, attendees will work through a practical recon methodology for identifying forgotten and abandoned hosts - using low-noise reconnaissance techniques available to any red teamer. We start together, walking through the methodology step by step against a prepared target modeled on patterns seen in real engagements. Then attendees get time to hunt independently while I'm available to answer questions. We close with a group debrief on what was found. A laptop with Kali, Parrot, or similar is recommended.

SpeakerBio: Yekaterina Shevchenko

Yekaterina Shevchenko is a Lead Security Testing Engineer focused on penetration testing and red teaming. She works on large-scope security assessments across complex environments, with an emphasis on repeatable workflows, clear evidence, and actionable remediation. Her experience covers infrastructure, web applications, and cloud security. Yekaterina also shares educational content under the nickname m0rn1ngstr on her YouTube channel, focused on practical offensive security topics.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Lonely Hackers Club - Saturday - 10:30-16:30 PDT

Title: Resume Review with the Lonely Hackers Club

Tags: Lonely Hackers Club | Creator Event/Activity

When: Saturday, Aug 8, 10:30 - 16:30 PDT

Where: LVCCW Level 1 Hall 4 1419 (Lonely Hackers Club) - [Map](#)

Description:

Free, one-on-one resume reviews, run by people from this community who have actually hired and managed technical teams. No recruiters. No corporate fluff. Just honest feedback from people who have sat on both sides of the table and know what works.

Sessions are 15 minutes. Walk up, sit down and get real feedback. Book your slot in advance or show up early to secure your spot if you missed the online registration.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Lonely Hackers Club - Friday - 10:30-16:30 PDT

Title: Resume Review with the Lonely Hackers Club

Tags: Lonely Hackers Club | Creator Event/Activity

When: Friday, Aug 7, 10:30 - 16:30 PDT

Where: LVCCW Level 1 Hall 4 1419 (Lonely Hackers Club) - [Map](#)

Description:

Free, one-on-one resume reviews, run by people from this community who have actually hired and managed technical teams. No recruiters. No corporate fluff. Just honest feedback from people who have sat on both sides of the table and know what works.

Sessions are 15 minutes. Walk up, sit down and get real feedback. Book your slot in advance or show up early to secure your spot if you missed the online registration.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Return of Sedinho: Current situation and new tactics of the Brazilian banking trojan ecosystem

Tags: Malware Village | Creator Talk/Panel

When: Friday, Aug 7, 13:15 - 13:55 PDT

Where: LVCCW Level 1 Hall 2 600 (Malware Village) Talks - [Map](#)

Description:

Last year we presented our research on the evolution of Brazilian banking trojans, their expansion into countries well beyond their original sphere of influence, and the law enforcement operations that attempted to disrupt their activity. Building on that work, this talk revisits the current landscape and examines the latest improvements and changes introduced by the malware operators behind these groups. In this session, we will analyze several recent financially motivated campaigns that show how Latin American threat actors are not only evolving classic banking malware, but also introducing NFC based mobile fraud against victims in multiple countries. We will provide concrete examples of how well known families such as Grandoreiro and Casbaneiro are refining both their techniques and their social engineering narratives while continuously adapting their malware infection chains and evasion strategies. We will also introduce their newest Android campaigns that leverage NFC fraud through a new NGate variant that masquerades as legitimate applications intended to relay NFC card data between devices. Cybercriminals distribute these trojanized apps under various pretexts, including online banking tools, lottery apps, and shopping applications. Once installed, the malware intercepts NFC payment card data and the victim's PIN, forwarding them to attacker controlled infrastructure to enable contactless ATM cash outs and fraudulent POS transactions, all without requiring additional risky permissions. Throughout the talk, we will walk through the observed tactics, techniques, and procedures, highlighting how the malware code, supporting infrastructure, and social engineering patterns have changed compared to the campaigns we analyzed previously. Our goal is to raise awareness of the ongoing evolution of these Latin American originated malware operations and to equip security teams with the context they need to detect and block these threats before they can cause damage to their organizations

SpeakerBio: Josep Albors, Head of Awareness & Research at Ontinet.com (ESET Spain)

Josep Albors is the Head of Awareness & Research at Ontinet.com (ESET Spain). He's a security expert with more than 21 years working in cybersecurity and specialized in security awareness. He is also the editor at the company's blog and one of the experts writing at several other publications related with the IT security world in Spain.

He has been a speaker at some of the most important security conferences in Spain, besides collaborating with initiatives such as X1RedMasSegura, that wants to raise awareness among users so they can use Internet and technology in a safe way. Included in Ontinet's social responsibility, Josep also does awareness and cybersecurity presentations in schools and universities. He's also a teacher in cyber security expert courses at several Spanish Universities and participates in several conferences organized by several spanish universities and Spain's national Institute of Cyber Security. He also participated as speaker at AVAR conference in Osaka in 2019, Caro Workshop 2023 in Bochum (Germany), FIRST 2024 (Fukuoka), Virus Bulletin 2024 (Dublín), Defcon Malware Village (2025), JSAC 2025 (Tokyo) and CARO 2026 (Innsbruck).

Josep has also collaborated with the Spanish Guardia Civil, Spanish National Police and the Spanish Army, teaching their units on how to fight cybercrime and with cyber intelligence training, contributing with his experience in analyzing cybercrime and malware.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Blacks In Cyber Village - Friday - 10:00-10:55 PDT

Title: Return of the Defender: Using AI to Strike Back Against Enterprise Threats

Tags: Blacks In Cyber Village | Creator Talk/Panel

When: Friday, Aug 7, 10:00 - 10:55 PDT

Where: LVCCW Level 3 W322-W324 (BIC Village) - [Map](#)

Description:

A long time ago, in a network not so far away attackers gained the upper hand. For years, enterprises have been on the defensive, overwhelmed by alerts, outpaced by automation, and outnumbered by adversaries using increasingly sophisticated tactics. But the balance of power is shifting. This is the Return of the Defender. AI is no longer just a tool it's becoming the force multiplier that allows security teams to reclaim control, respond faster, and anticipate threats before they strike. Join us to explore how AI is empowering defenders and learn strategies to reclaim control in the evolving threat landscape.

SpeakerBio: Levone Campbell, Chief Information Security Officer

Levone Campbell, MBA, MPS, CISSP

With more than two decades of experience in cybersecurity operations, Levone Campbell serves as a Cybersecurity Lead and Incident Coordinator, helping safeguard his organization's digital environment through strategic defense and incident response.

A seasoned information technology professional, Levone has developed deep expertise in cyber threat intelligence and cybercrime analysis, consistently anticipating and responding to emerging threats in an increasingly complex digital landscape. He has also expanded his focus to include the growing intersection of artificial intelligence and cybersecurity, with particular attention to the evolving challenges of AI-driven threats and defensive capabilities.

Levone's academic background includes dual bachelor's degrees in Management and Marketing from North Carolina A&T State University, a Master of Business Administration from Walden University, and a Master of Professional Studies in Technology Management with a concentration in Cybersecurity from Georgetown University.

His commitment to professional excellence is further demonstrated by his industry-recognized certifications, including the CISSP, which underscore his standing as a well-rounded cybersecurity leader.

Based in Houston, Texas, Levone values the balance between a demanding career and a strong family life. Married for 20 years and a proud father of two, he brings discipline, perspective, and purpose to his work in protecting critical digital assets and advancing cyber resilience.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Reversing a Recall: From 'Noise Triggered' to RCE

Tags: DEF CON Official Talk | Demo | Tool | Exploit

When: Sunday, Aug 9, 10:30 - 11:30 PDT

Where: LVCCW Level 1 Hall 3 904 (Main Track 4) - [Map](#)

Description:

Heavy-duty trucks move the majority of freight in North America, making them a critical component of our infrastructure. When a major supplier issued a recall to address a seemingly harmless noise issue, the explanation didn't quite add up.

This talk follows the reverse engineering journey that began with a simple question and led to a much larger discovery. By tearing apart firmware, analyzing the update protocols, and tracing ECU behavior, we uncovered evidence that the recall was not just remediating noise triggered flaws. Hidden within the recall's firmware update was a security mitigation addressing undisclosed vulnerabilities affecting a critical vehicle system.

Attendees will see how modern tractor ECUs can be analyzed using professional and public tools and techniques (IDA Pro, idapython, qbindiff), the challenges of working with the safety-critical microcontrollers in heavy-vehicles (S12XE), and the evidence that revealed security impacts of the patch. Along the way, we'll discuss the growing cybersecurity risks facing commercial vehicles.

Whether you're interested in automotive hacking, embedded systems, reverse engineering, or critical infrastructure security, this session offers a look inside the cybersecurity reality of the machines that keep the supply chain moving.

1. Aleph One. (1996). Smashing The Stack For Fun And Profit. *Phrack Magazine*, 7(49).
<http://phrack.org/issues/49/14.html>
2. Intellon Corporation. (1997). *SSC P485 PL Transceiver IC Data Sheet*.
3. Hunter, J. D. (2007). Matplotlib: A 2D graphics environment. *Computing in science & engineering*, 9(3), 90-95.
4. NXP Semiconductors. (2010). *HiWave Debugger*. Part of CodeWarrior Development Studio.
5. Krzywinski, M., Birol, I., Jones, S. J., & Marra, M. A. (2011). Hive plots—rational approach to visualizing networks. *Briefings in bioinformatics*, 13(5), 627-644.
6. SAE International. (2013). *J1587: Electronic Data Interchange Between Microcomputer Systems in Heavy-Duty Vehicle Applications*. Warrendale, PA.
7. Miller, C., & Valasek, C. (2014). *Adventures in Automotive Networks and Control Units*. IOActive.
https://www.ioactive.com/wp-content/uploads/pdfs/IOActive_Adventures_in_Automotive_Networks_and_Control_Units.pdf
8. Behere, S., Zhang, X., Izosimov, V., & Törngren, M. (2016). *A Functional Brake Architecture for Autonomous Heavy Commercial Vehicles*. <https://legacy.sae.org/publications/technical-papers/content/2016-01-0134/>
9. SAE International. (2016). *J1708: Serial Data Communications Between Microcomputer Systems in Heavy-Duty Vehicle Applications*. Warrendale, PA.
10. TruckHacking organization. (2016). *py-hv-networks*. <https://github.com/TruckHacking/py-hv-networks>
11. SAE International. (2018). *J1939: Serial Control and Communications Heavy Duty Vehicle Network*. Warrendale, PA.
12. International Organization for Standardization. (2018). *ISO 26262: Road vehicles -- Functional safety*. Geneva, Switzerland.
13. International Organization for Standardization. (2018). *ISO/IEC 29147: Information technology -- Security techniques -- Vulnerability disclosure*. Geneva, Switzerland.
14. dfieschko. (2019). *RP1210*. <https://github.com/dfieschko/RP1210>
15. MITRE Corporation. (2020). *CVE-2020-14514*. <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-14514>
16. International Organization for Standardization. (2020). *ISO 14229: Road vehicles -- Unified diagnostic services (UDS)*. Geneva, Switzerland.
17. Gardiner, B. (2022). Disclosure of confirmed remote write to J2497 aka PLC4TRUCKS. *NMFTA, Alexandria, VA, Letter, March*.

18. National Motor Freight Traffic Association. (2022). *Actionable Mitigations Options v9*.
https://nmfta.org/wp-content/media/2022/11/Actionable_Mitigations_Options_v9_DIST.pdf
19. MITRE Corporation. (2022). *CVE-2022-26131*. <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26131>
20. Pulse Security. (2022). *Reversing the Ducati 696 ECU Part 2*. <https://pulsesecurity.co.nz/articles/ducati-696-part2>
21. Gardiner, B. (2022). Mitigating PLC4TRUCKS Remote Write. *Proceedings of the 9th escar USA Conference*.
<https://escar.info/downloads>
22. Cybersecurity and Infrastructure Security Agency. (2023). *Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default*.
<https://www.cisa.gov/resources-tools/resources/shifting-balance-cybersecurity-risk-principles-and-approaches-security-des>
23. Bendix Commercial Vehicle Systems LLC. (2024). *24E086 Chronology*.
<https://static.nhtsa.gov/odi/rcl/2024/RMISC-24E086-5355.pdf>
24. National Highway Traffic Safety Administration. (2024). *Technical Service Bulletin 10194446*.
<https://dot.report/bulletins/10194446>
25. National Highway Traffic Safety Administration. (2024). *Technical Service Bulletin 10176745*.
<https://dot.report/bulletins/10176745>
26. National Highway Traffic Safety Administration. (2024). *Technical Service Bulletin 10222229*.
<https://dot.report/bulletins/10222229>
27. PACCAR Incorporated. (2024). *Safety Recall Report 24V-915*.
<https://static.nhtsa.gov/odi/rcl/2024/RCLRPT-24V915-6438.PDF>
28. Navistar, Inc. (2024). *Safety Recall Report 24V-818*. <https://static.nhtsa.gov/odi/rcl/2024/RCLRPT-24V818-4283.PDF>
29. Volvo Trucks North America. (2024). *Safety Recall Report 24V-790*.
<https://static.nhtsa.gov/odi/rcl/2024/RCLRPT-24V790-3386.PDF>
30. Bendix Commercial Vehicle Systems LLC. (2024). *Technical Bulletin TCH-27-007*.
https://www.bendix.com/media/services-and-support/product-action-center-pdfs/tch_27_007_en_000.pdf
31. Bendix Commercial Vehicle Systems LLC. (2024). *Technical Bulletin TCH-27-006*.
https://www.bendix.com/media/services-and-support/product-action-center-pdfs/tch_27_006_en_000.pdf
32. Bendix Commercial Vehicle Systems LLC. (2024). *Technical Bulletin TCH-27-008*.
https://www.bendix.com/media/services-and-support/product-action-center-pdfs/tch-27-008_en_000.pdf
33. ZF Friedrichshafen AG. (2024). *mBSP XBS Factsheet*.
https://www.zf.com/public/org/ZF_CVS_mBSP_XBS_Factsheet_EN_296135.pdf
34. Technology & Maintenance Council. (2024). *Position Paper 2024-3: Next Generation Tractor-Trailer Technical Needs*. American Trucking Associations.
https://tmc.trucking.org/sites/default/files/TMC_PP-2024_3_NEXTGEN_TRACTOR_TRAILER_TECHNICAL_NEEDS
35. Gardiner, B., Maag, J., & Tindell, K. (2024). *Security Requirements for Vehicle Security Gateways*. SAE International. <https://www.sae.org/papers/security-requirements-vehicle-security-gateways-2024-01-2806>
36. Vehicle Cybersecurity Working Group (VCRWG), National Motor Freight Traffic Association. (2024). *NMFTA Vehicle Cybersecurity Requirements*. https://github.com/nmfta-repo/nmfta-vehicle_cybersecurity_requirements
37. python-can Developers. (2024). *python-can*. <https://python-can.readthedocs.io/>
38. Cohen, R., David, R., Mori, R., Yger, F., & Rossi, F. (2024). Improving binary diffing through similarity and matching intricacies. *Proc. of the 6th Conference on Artificial Intelligence for Defense*.
39. Quarkslab. (2024). *Quokka*. <https://github.com/quarkslab/quokka>
40. Bendix Commercial Vehicle Systems LLC. (2025). *Safety Recall Report 25E-073*.
<https://static.nhtsa.gov/odi/rcl/2025/RCLRPT-25E073-3346.pdf>
41. National Motor Freight Traffic Association. (2025). *Bendix EC80 Recall: Safety and Security Implications*.
<https://nmfta.org/bendix-ec80-recall-safety-and-security-implications/>
42. Cybersecurity and Infrastructure Security Agency. (2025). *ICS Advisory (ICSA-25-021-03) Bendix EC-80*.
<https://www.cisa.gov/news-events/ics-advisories/icsa-25-021-03>
43. National Security Agency. (2025). *Ghidra*. <https://ghidra-sre.org/>
44. Hiveplotlib Developers. (2025). *hiveplotlib*. <https://github.com/hiveplotlib/hiveplotlib>
45. Land Line Media. (2025). *Defective Bendix ECUs have prompted recall of nearly half a million trucks with latest Paccar recall*.
<https://landline.media/defective-bendix-ecus-have-prompted-recall-of-nearly-half-a-million-trucks-with-latest-paccar-recall>
46. SAE Truck and Bus Control and Communications Network Committee. (2026). *J2497 Power Line Carrier Communications for Commercial Vehicles*. Work in Progress Draft Revision.
47. Hex-Rays. (2026). *IDA Pro*. <https://hex-rays.com/ida-pro/>

48. Python Software Foundation. (2026). *Python Programming Language*. <https://www.python.org/>
49. Graphviz Authors. (2026). *Graphviz*. <https://graphviz.org/>
50. ELDB. *XPROG-box*. <https://www.eldb.eu/>
51. PEmicro. *PROGS12Z Flash Programmer Software*. <https://www.pemicro.com/>
52. NXP Semiconductors. *MC9S12XEQ512 Data Sheet*. <https://www.nxp.com/docs/en/data-sheet/MC9S12XEP100.pdf>
53. NXP Semiconductors. *MC9S12XE Family Reference Manual*.
<https://www.nxp.com/docs/en/reference-manual/MC9S12XERM.pdf>
54. DARPA. *Assured Micropatching (AMP)*. <https://www.darpa.mil/program/assured-micropatching>
55. LinkerScope Developers. *LinkerScope*. Visualization Tool.
56. Zynamics. *BinDiff*. <https://www.zynamics.com/bindiff.html>
57. hotwolf. *HSW12*. <https://github.com/hotwolf/HSW12>
58. National Highway Traffic Safety Administration. *NHTSA Recalls by Manufacturer*.
<https://datahub.transportation.gov/Automobiles/NHTSA-Recalls-by-Manufacturer/mu99-t4jn>
59. Yapo, T. *FL2K Experiments*. <https://hackaday.io/project/164346-fl2k-sdr>
60. Osmocom. *Osmo-FL2k Project*. <https://osmocom.org/projects/osmo-fl2k>
61. National Highway Traffic Safety Administration. *Federal Motor Vehicle Safety Standard No. 121, Air Brake Systems*.
49 CFR 571.121.
62. Evenchick, E. *CANtact*. <https://cantact.io/>
63. National Motor Freight Traffic Association. *j2497-keyhole*. <https://github.com/nmfta-repo/j2497-keyhole>
64. Motorola. *Motorola S-Record Description (PDF)*.
https://deramp.com/downloads/mfe_archive/060-Standards%20and%20Specifications/Hex%20Data%20Formats/Motorola

SpeakerBio: Ben Gardiner, NMFTA Inc.

Ben is a Senior Cybersecurity Research Engineer contractor at the National Motor Freight Traffic Association, Inc.® (NMFTA)® specializing in hardware and low-level software security.

With more than ten years of professional experience in embedded systems design and a lifetime of hacking experience, Ben has a deep knowledge of the low-level functions of operating systems and the hardware with which they interface.

He has held security assurance and reversing roles at a global corporation, as well as worked in embedded software and systems engineering roles at several organizations.

Ben has conducted workshops and presentations at leading cybersecurity and technical mobility events globally, including Black Hat USA, DEF CON, NorthSec, escar USA, ScappyCon, the CyberTruck Challenge, GENIVI Security Sessions, Hack in Paris, and HackFest.

In addition to speaking on the main stage at Black Hat USA and DEF CON, Ben is a volunteer at the DEF CON Hardware Hacking Village (DC HHV) and Car Hacking Village (CHV). He is GIAC -GPEN, and -GICSP certified and a GIAC advisory board member, serves as the chair of the SAE TEVEES18A1 Cybersecurity Assurance Testing Task Force (responsible for J3322), a contributor to ATA TMC task forces, the ISO/SAE JWG and a voting member of the SAE VESS.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Reversing F5: Pure-Go Steganography, Live Forensic Cover Recovery, and JPEG Fragility Analysis

Tags: Intro/Beginner | AI | DEF CON Demo Labs | Cloud | Defense/Blue Team | Malware | Mobile | Offense/Red Team | Purple Team | SecOps | Threat Intel/Hunting | DEF CON Demo Labs

When: Saturday, Aug 8, 10:00 - 10:45 PDT

Where: LVCCW Level 1 Hall 3 901 (Demo Labs Track 5) - [Map](#)

Description:

F5 (Westfeld, 2001) is the canonical "do it right" JPEG steganography algorithm — matrix encoding, permutative straddling, shrinkage handling — and still turns up on confiscated devices and in CTF challenges 25 years later. The public tooling has rotted: the original is Java, modern rewrites bind CGo to libjpeg, and every implementation surveyed is one-way (embed and extract, never un-embed). This Demo Lab presents ten public GitHub repositories that fix that, in pure Go with zero third-party dependencies. The headline is the first open-source F5 cover-recovery tool: given the stego JPEG, the password, and the extracted message, it reverses the embed and restores the cover's DCT coefficients. Alongside it ship three CLIs (embed, extract, recover), a pure-Go JPEG-family codec (baseline, JPEG 2000, JPEG-LS, XL/XR/XS/XT, Pleno, lossless), a Fridrich chi-square steganalysis library and CLI, and the supporting crypto, i18n, and logging packages — all auditable end-to-end in one language. Live: embed, extract, cover recovery, defensive Fridrich detection, JPEG re-encoding fragility, and a 25-line external Go program importing the library. Useful for digital forensics, steganalysis research, CTF authoring, and anyone who wants a CGo-free stego stack they can read in a weekend.

SpeakerBio: Overkilll

Precise, Ruthless, Ethical

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Reversing F5: Pure-Go Steganography, Live Forensic Cover Recovery, and JPEG Fragility Analysis

Tags: Intro/Beginner | AI | DEF CON Demo Labs | Cloud | Defense/Blue Team | Malware | Mobile | Offense/Red Team | Purple Team | SecOps | Threat Intel/Hunting | DEF CON Demo Labs

When: Friday, Aug 7, 16:00 - 16:45 PDT

Where: LVCCW Level 1 Hall 3 901 (Demo Labs Track 5) - [Map](#)

Description:

F5 (Westfeld, 2001) is the canonical "do it right" JPEG steganography algorithm — matrix encoding, permutative straddling, shrinkage handling — and still turns up on confiscated devices and in CTF challenges 25 years later. The public tooling has rotted: the original is Java, modern rewrites bind CGo to libjpeg, and every implementation surveyed is one-way (embed and extract, never un-embed). This Demo Lab presents ten public GitHub repositories that fix that, in pure Go with zero third-party dependencies. The headline is the first open-source F5 cover-recovery tool: given the stego JPEG, the password, and the extracted message, it reverses the embed and restores the cover's DCT coefficients. Alongside it ship three CLIs (embed, extract, recover), a pure-Go JPEG-family codec (baseline, JPEG 2000, JPEG-LS, XL/XR/XS/XT, Pleno, lossless), a Fridrich chi-square steganalysis library and CLI, and the supporting crypto, i18n, and logging packages — all auditable end-to-end in one language. Live: embed, extract, cover recovery, defensive Fridrich detection, JPEG re-encoding fragility, and a 25-line external Go program importing the library. Useful for digital forensics, steganalysis research, CTF authoring, and anyone who wants a CGo-free stego stack they can read in a weekend.

SpeakerBio: Overkilll

Precise, Ruthless, Ethical

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Radio Frequency Village - Sunday - 12:00-12:55 PDT

Title: RF CTF and World Wide War Drive Outbrief

Tags: Radio Frequency Village | Radio Frequency Capture the Flag | Creator Talk/Panel

When: Sunday, Aug 9, 12:00 - 12:55 PDT

Where: LVCCW Level 1 Hall 1 409 (Radio Frequency Village) - [Map](#)

Description:

Final results of RF CTF announced!

SpeakerBio: RF Hackers, RF Hackers Sanctuary

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Radio Frequency Village - Friday - 10:30-12:25 PDT

Title: RF CTF Kick Off Day 1

Tags: Radio Frequency Village | Radio Frequency Capture the Flag | Creator Talk/Panel

When: Friday, Aug 7, 10:30 - 12:25 PDT

Where: LVCCW Level 1 Hall 1 409 (Radio Frequency Village) - [Map](#)

Description:

Presentation to kick off the Radio Frequency Village CTF with helpful tips for new folks.

SpeakerBio: RF Hackers, RF Hackers Sanctuary

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Radio Frequency Village - Saturday - 10:30-12:25 PDT

Title: RF CTF Kick Off Day 2

Tags: Radio Frequency Village | Radio Frequency Capture the Flag | Creator Talk/Panel

When: Saturday, Aug 8, 10:30 - 12:25 PDT

Where: LVCCW Level 1 Hall 1 409 (Radio Frequency Village) - [Map](#)

Description:

Presentation to kick off the Radio Frequency Village CTF with helpful tips for new folks.

SpeakerBio: RF Hackers, RF Hackers Sanctuary

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: RFID Bootcamp: Unleashed!

Tags: Red Team Village | Misc

When: Friday, Aug 7, 10:00 - 11:59 PDT

Where: LVCCW Level 1 Hall 1 309 (Red Team Village) Workshop Tactic Table 6 - [Map](#)

Description:

Are you ready for a high-octane sprint into RFID?

This isn't a sit-and-listen lecture with a few party tricks; it's a battle-tested 30-minute bootcamp to demystify RFID and unleash your skills. All levels welcome - It's time to blow the dust off your tools, and learn what has helped hundreds of other hackers get (and stay!) into RFID for good.

In this unleashed session, you will:

- Build a rock-solid understanding of how RFID actually works from card, to reader, to full scope system.
- Get hands-on with modern tools with live demos, learning tactics and mindsets - not just commands.
- Most importantly, learn how to build your own RFID lab to keep the learning going long after you leave DEFCON!

Led by Evan "Shortrange" Cook — RF trainer to hundreds and creator of the OpenDoorSim — this is a bootcamp you won't want to miss. All are welcome!

SpeakerBio: Evan Cook

Evan "Shortrange" Cook is a physical security researcher who specializes in turning locked doors into open opportunities. A first-place winner of the DEFCON 2025 Embedded Systems Village CTF and SAINTCON 2024 RFID CTF, Evan knows how to train and speak success in RFID hacking. He is a battle-tested educator who has workshoped over 300+ students — ranging from newbies to industry professionals to tier-one special forces operators — in the art of successful access control exploitation. Committed to lowering the barrier of entry for beginners, he created the world's FIRST open-source access control simulation lab built entirely with off-the-shelf parts, proving that high-end security research doesn't require a high-end budget. Evan is passionate about "bringing RFID to the people" through talks, workshops, trainings, and open-source projects. Where digital and physical worlds collide... you'll find Shortrange ready to "Hack the Planet!" with you.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Riding for Free - Breaking Public Transport RFID at Scale

Tags: DEF CON Official Talk | Demo | Exploit

When: Friday, Aug 7, 15:30 - 16:30 PDT

Where: LVCCW Level 1 Hall 3 904 (Main Track 4) - [Map](#)

Description:

How many of you tapped an RFID card to ride a train this year? How many of you know what's actually stored on it? Every transit authority in the world builds their own proprietary card formats, and not one has ever published a spec. The security model is the same everywhere: if nobody knows the format, nobody can exploit it. I spent two years testing that assumption. Across 50+ cities and every major contactless protocol, I reverse engineered the proprietary data formats that transit systems treat as their last line of defense. Along the way I built Metroflip, an open source transit card reader for the Flipper Zero, and found critical vulnerabilities in Spain's two largest transit systems that allow unlimited free travel. On RENFE, Spain's national rail, I cracked a proprietary checksum algorithm that lets you directly modify trip counters, expiry dates, and zones on any card in the country. On T-Mobilitat, Barcelona's modern encrypted metro platform, I bypassed card-level crypto entirely by changing a single byte in the mobile app's relay, getting free trips and automatic refunds. I'll walk through the methodology, demo the RENFE exploit live on stage with a Flipper Zero, and share some hard lessons about what happens when you try to responsibly disclose vulnerabilities in infrastructure you depend on every day.

Garcia, de Koning Gans, Muijters, van Rossum, Verdult, Schreur, Jacobs. "Dismantling MIFARE Classic." ESORICS 2008. <https://flaviidgarcia.com/publications/Dismantling.Mifare.pdf> Courtois, N. "The Dark Side of Security by Obscurity." 2009. Darkside attack on MIFARE Classic CRYPTO1. Anderson, Ryan, Chiesa. "Anatomy of a Subway Hack." DEF CON 16, 2008. (Boston CharlieCard) Rauch, B. "The Boston Infinite Money Glitch." DEF CON 31, 2023. Garcia, de Koning Gans, Verdult. "Wirelessly Pickpocketing a Mifare Classic Card." IEEE S&P 2009. NXP Semiconductors. "MIFARE DESFire EV2/EV3 Functional Specification." (restricted distribution) Wouters, Carroll. "Unsaflok: Hacking Millions of Hotel Locks." DEF CON 32, 2024. Rodriguez. "Contactless Overflow." DEF CON 31, 2023. Hunt, Nakache. "Hung Out to Dry: Airing the Dirty Laundry of Stored Value Washing Cards." 2025. Metrodroid project. <https://github.com/metrodroid/metrodroid> Metroflip project. <https://github.com/luu176/Metroflip> Proxmark3 RRG. <https://github.com/RfidResearchGroup/proxmark3> CRC RevEng catalogue. <https://reveng.sourceforge.io/crc-catalogue/>

SpeakerBio: Aidan "luu176" Nakache

Aidan Nakache is a 17-year-old CTO at dubblefilm, where he leads software and hardware development with a focus on automation, operational efficiency, security, and scalable growth. He develops and maintains company servers, hardware systems, and transaction equipment, with much of his work centered around fintech infrastructure, system expandability, and technology migration.

Alongside his role, he is a cybersecurity researcher and hardware hacker specializing in RFID, reverse engineering, and access-control systems. He enjoys competing in CTFs at conferences around the world and has spoken at DEF CON 33 in the Radio Frequency Hackers Sanctuary village. He shares open-source work on GitHub and continues to collaborate and grow within the field.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Game Hacking Village - Saturday - 10:00-16:59 PDT

Title: Riot Games Vanguard: Pwn to own

Tags: Game Hacking Village | Creator Event/Activity

When: Saturday, Aug 8, 10:00 - 16:59 PDT

Where: LVCCW Level 1 Hall 1 211 (Game Hacking Village) - [Map](#)

Description:

(Exact times TBD) Try your hand at hacking Riot Game's signature anti-cheat: Vanguard!

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Game Hacking Village - Friday - 12:00-16:59 PDT

Title: Riot Games Vanguard: Pwn to own

Tags: Game Hacking Village | Creator Event/Activity

When: Friday, Aug 7, 12:00 - 16:59 PDT

Where: LVCCW Level 1 Hall 1 211 (Game Hacking Village) - [Map](#)

Description:

(Exact times TBD) Try your hand at hacking Riot Game's signature anti-cheat: Vanguard!

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Game Hacking Village - Saturday - 10:00-10:45 PDT

Title: RIP Denuvo: DRM in a Post-Hypervisor World

Tags: Game Hacking Village | Creator Talk/Panel

When: Saturday, Aug 8, 10:00 - 10:45 PDT

Where: LVCCW Level 1 Hall 3 801 (Creator Stage 2) - [Map](#)

Description:

For a decade, Denuvo stood as the gold standard of game DRM. That reign has come to an abrupt end. Thanks to the advent of Hypervisor bypasses, games are now being cracked in a matter of hours rather than months. How did we get here, and what does the future hold for game DRM?

SpeakerBio: Amin Hussien

Amin Hussien is the co-creator of the Illusory Unreal Engine game modding community (<https://illusory.dev/>) and has previously worked as an anti-cheat developer at [Redacted].

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

The Diana Initiative - Friday - 10:40-10:50 PDT

Title: Robot Hacking Community Tour

Tags: The Diana Initiative | Creator Tour

When: Friday, Aug 7, 10:40 - 10:50 PDT

Where: LVCCW Level 1 South Lobby / Atrium - [Map](#)

Description:

Interested in visiting Robot Hacking Community but afraid to go by yourself? The Diana Initiative is hosting tours! Follow a volunteer to Robot Hacking Community and be introduced to the community and activities inside!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Blacks In Cyber Village - Saturday - 12:00-12:25 PDT

Title: Root Access: An APT Analysis of Systemic Gatekeeping in Cybersecurity

Tags: Blacks In Cyber Village | Creator Talk/Panel

When: Saturday, Aug 8, 12:00 - 12:25 PDT

Where: LVCCW Level 3 W322-W324 (BIC Village) - [Map](#)

Description:

Explore the unseen authorization systems shaping the cybersecurity field in this compelling talk. We'll apply threat intelligence and access control theory to understand who gains entry, who advances, and who sets the rules. Discover an APT architectural approach to visualize systemic gatekeeping and learn social-engineering strategies to gain 'root access.' The session will present two distinct threat models, inviting you to analyze the system as both an adversary and a target. Drawing on 30 years of experience and research in Next Generation Access Control (NGAC) hypergraph authorization, the speaker will equip attendees with a formal model for understanding the system, effective Tactics, Techniques, and Procedures (TTPs) to navigate it, and a framework for influencing the policies that govern our field. Don't miss this opportunity to gain critical insights and strategies for cybersecurity career navigation.

SpeakerBio: Dr. Hassan Karim, Stable Cyber LLC

Hassan Karim, PhD is a cybersecurity researcher, academic, and founder of Stable Cyber LLC, with over 30 years of experience spanning financial infrastructure and payment systems at Goldman Sachs and JPMorgan Chase, OT/SCADA security and nation-scale infrastructure design at Aramco, and risk engineering across PNC Bank and Comerica. They hold a PhD in Computer Science from Howard University and conduct research in formal authorization models, adversarial AI risk, and cyber-physical systems security. Their published work on hypergraph-based access control for agentic AI and multi-robot systems is the technical foundation for this talk. They have operated, navigated, and quietly reverse-engineered the systems this talk is about for three decades.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Root From Kilometers Away: Ubiquiti AirMax RCE

Tags: DEF CON Official Talk | Demo | Tool | Exploit

When: Saturday, Aug 8, 10:30 - 11:30 PDT

Where: LVCCW Level 1 Hall 3 904 (Main Track 4) - [Map](#)

Description:

You don't realize it until you see them; they're everywhere. From Wireless ISP links to the frontline of modern warfare. But nobody found anything? The devices behind those links are Ubiquiti AirMAX: critical infrastructure on a 17-year-old Linux kernel and a custom 802.11 extension built on "security by obscurity." So we took it apart. This talk covers our reverse engineering of the AirMAX protocol, AirOS, and the kernel modules behind this proprietary mode. It rides on 802.11 Information Elements that look encrypted, but we'll show why they aren't. What we found: two critical vulnerabilities (CVE-2026-21639, CVE-2026-21638) across airMAX AC, airMAX M, airFiber, and GigaBeam, over 50 devices. These are the bugs from the movies: Over-The-Air, unauthenticated, kernel-privilege RCE. No network access, just line of sight. They affect every AirMAX device ever shipped. We disclosed them through Ubiquiti's bug bounty program. The bugs were rated "Adjacent", except adjacent here means kilometers away. The same hardware can be turned around and pointed at the problem: we'll repurpose these devices as recon tools and release open-source software to locate AirMAX networks in the wild. This talk is about our journey, our tooling, and the state of security.

Speakers: Federico Kirschbaum, Gaston Aznarez

SpeakerBio: Federico Kirschbaum, FaradaySec

Federico Kirschbaum is a security researcher with over two decades of experience building tools and ecosystems for offensive security. He is the Co-Founder and VP of Research in Faraday Security, an open-source platform. He is also the Co-Founder of Ekoparty, Latin America's largest hacking conference, where he has helped shape the region's security research community for over 20 years.

SpeakerBio: Gaston Aznarez, FaradaySec

Gaston Aznarez is a Principal Security Researcher at Faraday Security, focused on IoT and embedded device vulnerability research, firmware reverse engineering, wireless protocol analysis, and hardware-level exploitation. He has presented at DEF CON, Black Hat and Ekoparty.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Root-as-a-Service: The Hidden Runtime of Azure AI Foundry

Tags: Cloud Village | Creator Talk/Panel

When: Sunday, Aug 9, 12:30 - 13:10 PDT

Where: LVCCW Level 3 W313 (Cloud Village Talks) - [Map](#)

Description:

Azure AI Foundry promises a simple serverless AI experience: upload models, run workflows, execute Python code, and Azure handles the rest.

But what actually happens behind the scenes when you run a serverless AI workload?

In this talk, we expose the hidden Azure-managed infrastructure powering Azure AI Foundry serverless workloads. Our research uncovered privileged Azure-managed runtimes that are completely invisible to customers, where user-controlled code executes as root, with host integration and Docker access exposed by default.

But that was only the beginning.

We also discovered that Azure AI workloads can obtain delegated cloud tokens through internal Azure ML token broker services. In our demo, we show how a serverless AI workload can leverage these trust relationships to access Azure resources far outside the AI workspace scope simply because the workflow creator had access to them.

As organizations increasingly trust serverless AI workloads with autonomous execution, such environments are rapidly becoming one of the cloud's newest and overlooked attack surfaces.

This talk reveals how attackers can abuse hidden trust relationships inside Azure AI runtimes, why most organizations are blind to these attack paths, and what defenders must do before AI runtimes become the next major cloud pivot point.

SpeakerBio: Shani Peled

Shani Peled is a Senior Cloud Security Researcher at CrowdStrike, specializing in offensive cloud and AI security research. She began her career in the Israeli Intelligence Corps, where she served as the only female hacker on her cyber defense team protecting critical infrastructure. After transitioning into offensive security, she spent years conducting red team operations against enterprise environments worldwide, including Fortune 500, Fortune 100, and Fortune 50 companies. Today, her research focuses on exposing hidden trust relationships, identity abuse paths, and emerging attack surfaces across modern cloud and AI platforms.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: ROP for the Web: Smuggling XSS, SQLi, and Web Shells Past Every WAF Using Compression Dictionaries

Tags: Advanced | AppSec Village | Creator Event/Activity

When: Sunday, Aug 9, 10:15 - 11:15 PDT

Where: LVCCW Level 1 Hall 2 604 (Appsec Village) Arsenal - [Map](#)

Description:

Compression Dictionary Transport (RFC 9842) shipped in Chrome 130+ in 2025. Any JavaScript asset designated as a dictionary becomes a set of gadgets an attacker can chain into responses that bypass signature-based WAFs and IDSes. gadget-scanner is the a tool to evaluate that surface: drop in a candidate dictionary and a payload, and it reports how much of the payload hides inside backreferences and how much leaks as literal bytes on the wire. At the table you will score real-world JS libraries as attack primitives, generate the DCB blob with `broccoli -D`, and watch the side-by-side: the raw bytes a WAF would see vs. the payload a browser would execute

SpeakerBio: alevsk

Lenin Alevski is a Full Stack Engineer and generalist with a lot of passion for Information Security. Currently working as a Security Engineer at Google. Lenin specializes in building and maintaining Distributed Systems, Application Security and Cloud Security in general. Lenin loves to play CTFs, contributing to open-source and writing about security and privacy on his personal blog <https://www.alevsk.com>.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Ropkit: Framework for Windows Kernel Code Execution under HVCI

Tags: Malware Village | Creator Talk/Panel

When: Saturday, Aug 8, 13:05 - 13:45 PDT

Where: LVCCW Level 1 Hall 2 600 (Malware Village) Talks - [Map](#)

Description:

The Windows Kernel has become a highly hardened environment. With the default enforcement of HVCI (Hypervisor enforced Code Integrity), meaningful impacts of BYOVD (Bring your own vulnerable driver) attacks becomes increasingly difficult. Furthermore, modern BYOVD attacks require the use of physical read/write primitives, which leave the much more common virtual read/write primitives difficult to weaponize.

To assist in kernel exploitation, I developed two novel methods of kernel code execution within Windows given a virtual read/write primitive. I implemented PTE remapping that results an SSDT hijack, and a JOP chain that bypasses Kernel Shadow Stacks. These methods can only be blocked by hardware controls that are not yet implemented on AMD machines (Intel VT-rp), or are simply nonpresent in current Windows kernel (Kernel Shadow Stack Branch Tracking).

Additionally, I will be releasing ropkit, a dynamic kernel framework built to conduct BYOVD attacks. This framework functions on different windows builds with different drivers. Known and novel code execution methods are included into this framework as well. Red Teamers simply provide a driver exploit, and this framework automates the rest of the exploitation process.

SpeakerBio: Nathan Sawyer, Independent Researcher

Nathan Sawyer is a junior studying Cybersecurity at the University of Idaho. He has obtained HTB CDSA and CPTS. He enjoys skiing, snowboarding, hockey, and lacrosse.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Running a homelab with NixOS

Tags: Nix Vegas Community | Creator Talk/Panel

When: Friday, Aug 7, 11:30 - 11:59 PDT

Where: LVCCW Level 1 Hall 4 1310 (Nix Vegas Community) - [Map](#)

Description:

Are you looking to own your media again and host it for the family using NixOS? Some learn about doing that on your own hardware!

This presentation will cover the basics for NixOS Modules that are also used for these services in nixpkgs. It will also include examples of my configuration files hosted here:

<https://gitlab.com/ahoneybun/nix-configs>

Presentation includes showing my setup including how I handle the data in a RAID.

SpeakerBio: Aaron Honeycutt

a computer nerd who happens to use Linux



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Radio Frequency Village - Friday - 13:00-13:59 PDT

Title: Running your own LTE network for fun and profit???

Tags: Radio Frequency Village | Creator Talk/Panel

When: Friday, Aug 7, 13:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 3 1102 (Creator Stage 6) - [Map](#)

Description:

Running your own LTE network for fun and profit

This presentation will cover the journey from zero to dial tone on an fully legal OTA LTE network. We'll cover the equipment (both enodeB, user equipment, and sim cards), software stack (LTE Core, VoLTE services, e-sims), licensing and permitting requirements, how to bridge our network into SS7/POTS, and with any luck include a live demonstration of a call between phones connected to Lozaning-Tel.

We'll also briefly get into the the myriad ways with which we can leverage our privileged position as a trusted network operators to invalidate mobile security assumptions.

SpeakerBio: Lozaning

Lozaning (they/them) has been wardriving for over 10 years and enjoys designing, building, and assembling unorthodox network observation platforms such as: The Wifydra , The International Wigle Space Balloon, and turning an Amtrak roomette into a mobile radio observation lab. Lozaning loves all things wifi and high precision GNSS related, and is starting to maybe figure out BLE.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: SADF: A Taxonomy and Evaluation Framework for Agentic Security Failures

Tags: AI Village | Creator Talk/Panel

When: Saturday, Aug 8, 17:30 - 17:59 PDT

Where: LVCCW Level 1 Hall 3 801 (Creator Stage 1) - [Map](#)

Description:

Emerging agentic systems operate across attack surfaces that existing security evaluations were not designed to measure: external tools, persistent memory, retrieval pipelines, delegated credentials, and multi-agent orchestration. Most agent security benchmarks measure success using substring matching — checking whether attack-related keywords appear anywhere in the model response. We show this systematically overstates success rates because capable models quote attack indicators verbatim in their refusals.

We introduce SADF (Synthetic Agent Deception Framework), an eight-class taxonomy of agentic security failures — Tool Call Hijacking, Output Poisoning, Cross-Tool Injection, Memory Poisoning, RAG Poisoning, Delegated Authority Abuse, Multi-Agent Propagation, and Context Boundary Violation — and an automated testing harness with refusal-filtered scoring grounded in actual tool execution output strings.

Since the initial submission, we extended the evaluation from 3 direct model architectures to 7 total, adding four production framework wrappers (LangChain, AutoGen, CrewAI, SmolAgents), growing the dataset from 96 to 2,656 real evaluation runs. This extended evaluation reveals a finding absent from the original submission: the orchestration framework is an independent attack surface. Holding the model constant (Claude Sonnet) and varying only the framework wrapper produces a 2.6× spread in Agent Compromise Rate — from 11.9% (CrewAI) to 31.1% (SmolAgents) — with the direct Sonnet baseline at 15.6%. The choice of framework matters as much as the choice of model.

The original direct-model findings are confirmed and extended. Naive substring matching reported 90–100% success across all models; after refusal-filtered scoring, true rates were 59% (Llama 3.2), 22% (Claude Haiku), and 16% (Claude Sonnet) — a 4–6× overstatement. Memory Poisoning remains the sharpest safety boundary: Llama 3.2 was compromised on 3/3 payloads; all four framework architectures and Claude Sonnet achieved 0% across 243 combined Memory Poisoning runs. Delegated Authority Abuse scored 0% on both Claude models even when every authorization check passed — suggesting safety training captures intent, not only surface features. Two payloads (File Path Traversal, Code Execution to File Write) succeeded across all seven architectures, indicating a universal floor that neither safety training nor per-tool authorization controls currently address.

Attendees will leave with the full eight-class taxonomy, refusal-filtered scoring methodology, cross-architecture results across 2,656 real evaluation runs, and the complete open-source harness at github.com/jbdu94/SADF.

SpeakerBio: Julie Brunias

Julie Brunias is a cybersecurity professional with over 14 years of experience in offensive security, red teaming, and enterprise security architecture across sectors including energy, banking, telecommunications, and manufacturing. She specializes in AI security and adversarial system analysis, focusing on how generative AI systems, large language models, and agent-based architectures can be attacked, misused, and secured in real-world environments. Her work bridges offensive security and emerging AI system risks, including prompt injection, indirect prompt injection, RAG poisoning, model manipulation, and AI agent exploitation.

Julie has led red and purple team engagements and security architecture initiatives in complex enterprise environments, applying offensive security techniques to emerging AI-native systems and autonomous technologies.

Her research focuses on AI system failure modes, adversarial machine learning, Shadow AI risks, and practical methods for evaluating and securing agentic AI systems. She is the creator of several applied research efforts, including SADF (a taxonomy for agentic security failures), MCP security tooling, and ransomware intelligence analysis systems.

Her work has been presented at international security conferences including AI Village (accepted talk and poster), InCyber Forum, GoSec, HackMiami, and Black Hat (accepted), focusing on the intersection of offensive security and AI system resilience.

She is particularly focused on helping organizations understand and mitigate risks in production AI systems as they transition from experimental deployments to mission-critical infrastructure.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Safe, Secure, and Effective: What Static Behavior Analysis Reveals About the Software Running Your Medical Devices

Tags: Biohacking Village | Creator Talk/Panel

When: Saturday, Aug 8, 13:00 - 13:30 PDT

Where: LVCCW Level 1 Hall 3 1104 (Creator Stage 4) - [Map](#)

Description:

When a patient monitor misreads an ECG or an infusion pump miscalculates a dose, the root cause is software behavior, not a CVE. Yet the entire medical device security industry is fixated on vulnerability scanning and SBOMs while ignoring the harder question the FDA actually asks: does this software behave in ways that are safe and effective for its clinical purpose?

Using automated reverse engineering developed under ARPA-H research, we analyze compiled medical device firmware to build Software Bills of Behaviors that map what every function in a binary actually does. We automatically categorize hundreds of functions into clinical subsystems: ECG data processing, SpO2 and CO2 signal handling, physiological waveform display, sensor calibration, and heatblock control. We then identify which subsystems constitute essential performance, the functions where a bug, an unexpected change, or a malicious modification doesn't just create a cyber incident, it harms a patient.

We'll walk through real device firmware where we found functions that directly modify ECG configuration and hardware calibration state, where logic flaws or race conditions could impact device safety, stability, or data integrity. We'll show how a firmware update that only touches 10% of functions can silently alter safety-critical signal processing paths, and how we automatically assess whether those changes affect clinical operation or are benign. We'll demonstrate how the Contec CMS8000 patient monitor contained unapproved wireless monitoring capabilities the FDA never cleared, a safety and regulatory violation invisible to any vulnerability scanner.

Whether you're building devices, securing hospitals, or hacking medical firmware, this talk shifts the frame from "is it vulnerable?" to "is it safe?" because the patient on the other end doesn't care about your CVSS score.

SpeakerBio: Andrew Hendela

Andrew Hendela has been automating hard offensive and defensive cyber for well over a decade and a half, from VR, malware analysis, and cyber attribution. He is also a co-founder of Karambit.AI, a startup focused on validating the safety, security, and effectiveness of software and firmware.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Noob Community - Friday - 10:00-17:59 PDT

Title: SANS Institute NetWars Labs

Tags: Noob Community | Creator Event/Activity

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 4 1417 (Noob Community) - [Map](#)

Description:

SANS NetWars is a suite of advanced cyber ranges offering interactive, hands-on learning exercises created by SANS faculty in realistic network environments, gamifying cybersecurity training through compelling storylines and real-world challenges. Drop in during village hours to work through NetWars challenges at your own pace.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Noob Community - Saturday - 10:00-17:59 PDT

Title: SANS Institute NetWars Labs

Tags: Noob Community | Creator Event/Activity

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 4 1417 (Noob Community) - [Map](#)

Description:

SANS NetWars is a suite of advanced cyber ranges offering interactive, hands-on learning exercises created by SANS faculty in realistic network environments, gamifying cybersecurity training through compelling storylines and real-world challenges. Drop in during village hours to work through NetWars challenges at your own pace.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Noob Community - Sunday - 10:00-13:59 PDT

Title: SANS Institute NetWars Labs

Tags: Noob Community | Creator Event/Activity

When: Sunday, Aug 9, 10:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 4 1417 (Noob Community) - [Map](#)

Description:

SANS NetWars is a suite of advanced cyber ranges offering interactive, hands-on learning exercises created by SANS faculty in realistic network environments, gamifying cybersecurity training through compelling storylines and real-world challenges. Drop in during village hours to work through NetWars challenges at your own pace.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Aerospace Village - Friday - 10:00-17:59 PDT

Title: Satellites Under Attack: Hands-On Satellite Security Threat Scenarios

Tags: Aerospace Village | Creator Event/Activity

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 2 700 (Aerospace Village) - [Map](#)

Description:

In this “Satellite Attack Lab” you can explore how cyber-attacks against satellite systems can be launched, observed, and understood through a hands-on, attacker-centric experience. Rather than focusing on normal satellite operations, you will step into the role of a threat actor and directly exploit vulnerabilities in a simulated space environment by interacting with a physical setup of model satellites and ground stations to witness the immediate consequences of malicious actions, including intercepted data, unauthorized command execution, and visible disruption of satellite behavior.

We provide hacker workstations pre-configured with satellite command tools and signal-processing software. Large displays show the victim system’s telemetry and status in real time, allowing participants to immediately see the effects of their attacks.

This session is designed to be highly interactive and accessible to newcomers while still offering meaningful technical depth for advanced attendees.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Aerospace Village - Sunday - 10:00-13:59 PDT

Title: Satellites Under Attack: Hands-On Satellite Security Threat Scenarios

Tags: Aerospace Village | Creator Event/Activity

When: Sunday, Aug 9, 10:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 2 700 (Aerospace Village) - [Map](#)

Description:

In this “Satellite Attack Lab” you can explore how cyber-attacks against satellite systems can be launched, observed, and understood through a hands-on, attacker-centric experience. Rather than focusing on normal satellite operations, you will step into the role of a threat actor and directly exploit vulnerabilities in a simulated space environment by interacting with a physical setup of model satellites and ground stations to witness the immediate consequences of malicious actions, including intercepted data, unauthorized command execution, and visible disruption of satellite behavior.

We provide hacker workstations pre-configured with satellite command tools and signal-processing software. Large displays show the victim system’s telemetry and status in real time, allowing participants to immediately see the effects of their attacks.

This session is designed to be highly interactive and accessible to newcomers while still offering meaningful technical depth for advanced attendees.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Aerospace Village - Saturday - 10:00-17:59 PDT

Title: Satellites Under Attack: Hands-On Satellite Security Threat Scenarios

Tags: Aerospace Village | Creator Event/Activity

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 2 700 (Aerospace Village) - [Map](#)

Description:

In this “Satellite Attack Lab” you can explore how cyber-attacks against satellite systems can be launched, observed, and understood through a hands-on, attacker-centric experience. Rather than focusing on normal satellite operations, you will step into the role of a threat actor and directly exploit vulnerabilities in a simulated space environment by interacting with a physical setup of model satellites and ground stations to witness the immediate consequences of malicious actions, including intercepted data, unauthorized command execution, and visible disruption of satellite behavior.

We provide hacker workstations pre-configured with satellite command tools and signal-processing software. Large displays show the victim system’s telemetry and status in real time, allowing participants to immediately see the effects of their attacks.

This session is designed to be highly interactive and accessible to newcomers while still offering meaningful technical depth for advanced attendees.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: SBOM Find the Flaws

Tags: AppSec Village | Creator Event/Activity | All Audiences

When: Saturday, Aug 8, 11:00 - 12:59 PDT

Where: LVCCW Level 1 Hall 2 604 (Appsec Village) POD 4 - [Map](#)

Description:

SBOM Find the Flaws is a short hands-on activity where participants review SBOM files and identify intentional mistakes in the data, learning how to recognize common issues in software supply-chain documentation.

SpeakerBio: Dmitry Raidman

Dmitry Raidman is the Co-Founder and CTO of CyBeats, where he leads product and technology strategy focused on software supply chain security, SBOM management, and product security compliance. He works with organizations across regulated industries to operationalize SBOMs, improve software transparency, and manage vulnerability and third-party component risk at scale.

Dmitry is also active in the cybersecurity community, contributing to initiatives around AI security, SBOM adoption, and software supply chain risk. He is involved with the OWASP GenAI Security Project and the AIBOM Initiative, helping advance practical approaches for documenting and managing AI-related software and model supply chain exposure.

His work focuses on helping organizations move beyond checklist compliance toward measurable product security capabilities, continuous visibility, and faster response to emerging software and supply chain threats.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: SBOM Find the Flaws

Tags: AppSec Village | Creator Event/Activity || All Audiences

When: Saturday, Aug 8, 15:00 - 16:59 PDT

Where: LVCCW Level 1 Hall 2 604 (Appsec Village) POD 1 - [Map](#)

Description:

SBOM Find the Flaws is a short hands-on activity where participants review SBOM files and identify intentional mistakes in the data, learning how to recognize common issues in software supply-chain documentation.

SpeakerBio: Dmitry Raidman

Dmitry Raidman is the Co-Founder and CTO of CyBeats, where he leads product and technology strategy focused on software supply chain security, SBOM management, and product security compliance. He works with organizations across regulated industries to operationalize SBOMs, improve software transparency, and manage vulnerability and third-party component risk at scale.

Dmitry is also active in the cybersecurity community, contributing to initiatives around AI security, SBOM adoption, and software supply chain risk. He is involved with the OWASP GenAI Security Project and the AIBOM Initiative, helping advance practical approaches for documenting and managing AI-related software and model supply chain exposure.

His work focuses on helping organizations move beyond checklist compliance toward measurable product security capabilities, continuous visibility, and faster response to emerging software and supply chain threats.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: SBOM Find the Flaws

Tags: AppSec Village | Creator Event/Activity || All Audiences

When: Sunday, Aug 9, 11:00 - 12:59 PDT

Where: LVCCW Level 1 Hall 2 604 (Appsec Village) POD 3 - [Map](#)

Description:

SBOM Find the Flaws is a short hands-on activity where participants review SBOM files and identify intentional mistakes in the data, learning how to recognize common issues in software supply-chain documentation.

SpeakerBio: Dmitry Raidman

Dmitry Raidman is the Co-Founder and CTO of CyBeats, where he leads product and technology strategy focused on software supply chain security, SBOM management, and product security compliance. He works with organizations across regulated industries to operationalize SBOMs, improve software transparency, and manage vulnerability and third-party component risk at scale.

Dmitry is also active in the cybersecurity community, contributing to initiatives around AI security, SBOM adoption, and software supply chain risk. He is involved with the OWASP GenAI Security Project and the AIBOM Initiative, helping advance practical approaches for documenting and managing AI-related software and model supply chain exposure.

His work focuses on helping organizations move beyond checklist compliance toward measurable product security capabilities, continuous visibility, and faster response to emerging software and supply chain threats.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: SBOM Find the Flaws

Tags: AppSec Village | Creator Event/Activity || All Audiences

When: Friday, Aug 7, 15:00 - 16:59 PDT

Where: LVCCW Level 1 Hall 2 604 (Appsec Village) POD 3 - [Map](#)

Description:

SBOM Find the Flaws is a short hands-on activity where participants review SBOM files and identify intentional mistakes in the data, learning how to recognize common issues in software supply-chain documentation.

SpeakerBio: Dmitry Raidman

Dmitry Raidman is the Co-Founder and CTO of CyBeats, where he leads product and technology strategy focused on software supply chain security, SBOM management, and product security compliance. He works with organizations across regulated industries to operationalize SBOMs, improve software transparency, and manage vulnerability and third-party component risk at scale.

Dmitry is also active in the cybersecurity community, contributing to initiatives around AI security, SBOM adoption, and software supply chain risk. He is involved with the OWASP GenAI Security Project and the AIBOM Initiative, helping advance practical approaches for documenting and managing AI-related software and model supply chain exposure.

His work focuses on helping organizations move beyond checklist compliance toward measurable product security capabilities, continuous visibility, and faster response to emerging software and supply chain threats.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Scaling Adversary Emulation with Autonomous Agents

Tags: AI Village | Creator Talk/Panel

When: Sunday, Aug 9, 10:30 - 10:59 PDT

Where: LVCCW Level 1 Hall 3 1103 (Creator Stage 5) - [Map](#)

Description:

Manual red teaming cannot keep pace with modern enterprise attack surfaces, but autonomous agentic red teams offer a scalable alternative. In this talk we will present our experience and results on how to build and safely deploy offensive AI agents to conduct continuous, multi-stage adversary simulations at large scale to discover severe security issues and execute simulated post-exploitation chains.

SpeakerBio: Daniel Fabien

Daniel built Google's Red Team and ML Red Team from the ground up. He and his team of hackers conduct accurate simulations of real-world adversaries targeting the company, and use the lessons from these exercises to develop new defensive strategies. Prior to joining Google, Daniel worked as a pentester, helping companies identify and fix security vulnerabilities.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Scambait Village - Sunday - 10:00-13:59 PDT

Title: Scambait Bingo

Tags: Scambait Village | Creator Event/Activity

When: Sunday, Aug 9, 10:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 1 208 (Scambait Village) - [Map](#)

Description:

A fun, interactive group activity that turns classic bingo into a scambaiting game. Mark off common scam phrases, tactics, and red flags as they come up in curated recordings of real scam calls. Great for all skill levels, whether you are playing along or just hanging out. A low-pressure way to learn the language of scams while spending a few hours with the community. Prize-free by design. Winners get a certificate printed on the spot with a ridiculous honorific and a photo with village staff. Nothing of material value is awarded.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

The Diana Initiative - Saturday - 13:40-13:50 PDT

Title: Scambait Community Tour

Tags: The Diana Initiative | Creator Tour

When: Saturday, Aug 8, 13:40 - 13:50 PDT

Where: LVCCW Level 1 South Lobby / Atrium - [Map](#)

Description:

Interested in visiting Scambait Community but afraid to go by yourself? The Diana Initiative is hosting tours! Follow a volunteer to Scambait Community and be introduced to the community and activities inside!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

.EDU Community - Friday - 13:00-13:59 PDT

Title: ScamBusters: Turning Undergrads into Threat Hunters

Tags: .EDU Community | Creator Talk/Panel

When: Friday, Aug 7, 13:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 4 1418 (.EDU Community) - [Map](#)

Description:

SpeakerBio: Angela "BlondeTechie" Ramos

Angela Ramos is a University of Tampa cybersecurity lecturer. She leads the Scam Busters student program, coach for Trace Labs Search Party CTFs, and volunteers with US Cyber Games. She holds the GCIH, GSLC, and CEH certifications and spent a decade in DoD cyber operations.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Scambait Village - Saturday - 12:30-13:59 PDT

Title: Scammers Don't Discriminate

Tags: Scambait Village | Creator Talk/Panel

When: Saturday, Aug 8, 12:30 - 13:59 PDT

Where: LVCCW Level 1 Hall 1 208 (Scambait Village) - [Map](#)

Description:

Scammers don't just target the elderly. Young people are increasingly in their crosshairs. In this talk, DolphinVG examines how fraudsters are adapting their tactics to exploit youth through social media, gaming platforms, crypto schemes, job scams, romance scams, and more. Drawing on real cases and community experience, the session highlights why younger generations are vulnerable, the unique pressures they face, and practical ways the scambait community can help protect them.

SpeakerBio: DolphinVG

No BIO available

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Maritime Hacking Village - Friday - 14:15-14:45 PDT

Title: Scuttling Dashboards

Tags: Maritime Hacking Village | Creator Talk/Panel

When: Friday, Aug 7, 14:15 - 14:45 PDT

Where: LVCCW Level 1 Hall 3 801 (Creator Stage 2) - [Map](#)

Description:

The goldrush for maritime digitalization is riddled with safety concerns. Dashboards in the cloud stream vessel telemetry to shore-side consumers, and control planes from the cloud convey shore-side commands to shipboard IoT and OT systems. Systems of this nature involve an interaction between web applications, cloud, software defined networking systems, VPNs & OT systems, and are notoriously difficult to secure. This talk will showcase some of our research on these systems. From remote (over the internet) writes to propulsion / ballast systems, to turning a fleet of 300 ships into a botnet, we will discuss the possibilities of weaponization of maritime automation as demonstrated by first hand research.

SpeakerBio: Karan Sajnani, Rudra

Karan Sajnani is an entrepreneur and cybersecurity researcher, and the Founder and CEO of Rudra, a deep-tech firm building shipboard networking and security platforms deployed across more than 1,500 vessels globally. His work is grounded in hands-on vulnerability research, with multiple high-impact security disclosures across critical systems. Beyond maritime, his experience spans securing critical infrastructure in power and energy, RF systems, Telecom, as well as complex environments in financial services. Karan brings a practitioner's perspective to cybersecurity, focused not on theory or compliance, but on real-world attack paths and engineering-driven defense.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Social Engineering Community Village - Friday - 15:30-16:59 PDT

Title: SE Improv

Tags: Social Engineering Community Village | Creator Event/Activity

When: Friday, Aug 7, 15:30 - 16:59 PDT

Where: LVCCW Level 3 W320 (Social Engineering Community Village Labs) - [Map](#)

Description:

Join Kevin and Bryan from Black Box Improv Security for more hands-on activities putting their approach to improv theater to work in social engineering. Following their main-room lunchtime presentation on how improv skills can make or break an SE engagement, they will host a workshop in the SEC Labs that will include chances for participants to immediately put what they learn into practice. There will be games, there will be prizes, and there will inevitably be lots of laughs. There will also be the return of some favorite activities from previous years, including the One-Word Story Competition and Improvised Cold Calls. Attendee participation will not be mandatory, though it is always encouraged.

Speakers: Bryan, Kevin

SpeakerBio: Bryan

No BIO available

SpeakerBio: Kevin

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: search_vulns: Navigating the Fragmented Landscape of Vulnerability Data

Tags: AppSec Village | Creator Event/Activity | All Audiences

When: Sunday, Aug 9, 11:30 - 12:30 PDT

Where: LVCCW Level 1 Hall 2 604 (Appsec Village) Arsenal - [Map](#)

Description:

Due to advances in AI assisted vulnerability discovery, more vulnerabilities are published than ever before, while traditional aggregators like the NVD have long reached their limits. This makes it increasingly difficult to obtain reliable information for prioritization in the fragmented landscape of known vulnerability data. Our open-source tool, search_vulns, addresses this by consolidating various sources through a modular architecture that works with product identifiers, like CPEs or PURLs, and regular product banners. It maintains accuracy when incorporating data without CPEs or PURLs, derives valid CPEs when upstream data is incomplete and reconciles duplicate product identities. Ultimately, it delivers a unified and precise view of known vulnerabilities, exploits, KEV, software recency and backpatch information, which we believe outperforms similar solutions.

Speakers: Dustin Born, Matthias Göhring

SpeakerBio: Dustin Born

Dustin Born is security consultant and penetration tester at usd AG, an information security company based in Germany with the mission #moresecurity. Within pentesting, he focuses on web applications, cloud environments and mobile applications. Apart from this, Dustin supports the development of several internal tools that focus on automated reconnaissance and vulnerability assessment. This aligns with his interests in developing tools related to IT security and his previous scientific work. Specifically, he has built a framework for a general purpose vulnerability scanner as well as one for the dynamic analysis of iOS apps.

SpeakerBio: Matthias Göhring

Matthias Göhring is security consultant and penetration tester at usd AG, an information security company based in Germany with the mission #moresecurity. He is Head of usd HeroLab, the division of usd specialized in technical security assessments. In addition, he holds lectures at Technical University Darmstadt and University of Applied Sciences Darmstadt on ethical hacking and penetration testing. In previous scientific work, he focused on network and communication security as well as software security.

Previous publications: - Catching the Clones – Insights in Website Cloning Attacks, Risk Connect Conference, 2021 - Path MTU Discovery Considered Harmful, IEEE 38th International Conference on Distributed Computing Systems (ICDCS), 2018 - Tor Experimentation Tools, IEEE Security and Privacy Workshops, 2015 - On randomness testing in physical layer key agreement, IEEE 2nd World Forum on Internet of Things (WF-IoT), 2015

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Contests - Friday - 09:00-11:59 PDT

Title: SEC Vishing Competition (SEVC)

Tags: Social Engineering Community Village | Contest

When: Friday, Aug 7, 09:00 - 11:59 PDT

Where: LVCCW Level 3 W317-319 (Social Engineering Community Village) - [Map](#)

Description:

The official DEF CON contest SEVC is back, baby! Watch as teams turn months of research and rehearsal into live calls, matching sharp scripts against real corporate defenses for the win. This year's contest is judged this year by Snow, Jayson E. Street, and Kimberley Mitnick.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Contests - Friday - 13:00-15:59 PDT

Title: SEC Vishing Competition (SEVCV)

Tags: Social Engineering Community Village | Contest

When: Friday, Aug 7, 13:00 - 15:59 PDT

Where: LVCCW Level 3 W317-319 (Social Engineering Community Village) - [Map](#)

Description:

Now after our improv break, more teams place live calls, putting polished scripts and fresh research to the test against real corporate defenses in the SEVCV! Should out this year years coaches: JC, Jenn, Shadow Fox, and Hall&OSINT.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Social Gatherings/Events - Friday - 22:00-00:59 PDT

Title: SecKC the WHOLE WIDE WORLD

Tags: Party

When: Friday, Aug 7, 22:00 - 00:59 PDT

Where: LVCCW Level 1 North Lobby - [Map](#)

Description:

Following the legendary chaos of SecKC the World and SecKC the World Again, the Kansas City crew returns to DEF CON to settle the digital frontier. This year, we aren't just hosting a party, this isn't just another loud room with a DJ; it's gonna be a killer getogether for the hacker family. We're merging the independent spirit of the DEF CON with the radical community of the Midwest.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: SecretSifter: Production Apps Are Leaking Credentials. The Blindspot DAST Never Checked.

Tags: DEF CON Demo Labs | Intermediate | AppSec | Defense/Blue Team | DevOps | Offense/Red Team | Threat Intel/Hunting | DEF CON Demo Labs

When: Friday, Aug 7, 14:00 - 14:45 PDT

Where: LVCCW Level 1 Hall 3 1001 (Demo Labs Track 1) - [Map](#)

Description:

Shift-left tools scan what you commit, not what you serve. DAST scanners test for vulnerabilities but ignore live traffic. The industry left a gap: runtime secrets. Finding them requires intercepting live traffic: a proxy, a browser extension, or a bulk scanner. SecretSifter is all three.

We tested 2,000 production apps against ten secret scanners. 194 confirmed credentials survived all ten scanners.

SecretSifter monitors live HTTP traffic and finds credentials in JS bundles, lazy-loaded chunks, HTML responses, JSON and XML APIs, and request headers. No config, no source code. 160+ rules cover vendor tokens (AWS, Azure, Stripe, Twilio, GitHub), entropy-gated patterns, and CryptoJS-encrypted configs where the decryption key is hardcoded in the same bundle. No other scanner catches that case. Bulk mode scans 30-50 targets: paste URLs, scan, optional AI triage, export HTML, CSV, or ZIP.

The session opens with a live tool comparison. Most tools scan one URL at a time and require manual browsing. SecretSifter bulk-scans both targets in parallel. Two findings none of the ten caught: Azure AD credentials baked into a webpack bundle past GitLeaks. A CryptoJS config with the decryption key three lines away.

Your entire pipeline reported green. Were they right? Attendees leave with a free tool to run the same day.

SpeakerBio: Hemanth Gorijala

Hemanth Gorijala is Global Pentest Lead at a Fortune 100 financial services company. He built SecretSifter to close the runtime security gap: the space between where shift-left secret scanning stops and where secrets actually appear in production. His research identified 194 confirmed credentials across 2,000 production applications that bypassed ten secret scanners. He is presenting that research at security conferences across the US. The GT-194 benchmark is published on Zenodo (DOI 10.5281/zenodo.19464446). SecretSifter is open source at github.com/secretsifter.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: SecretSifter: Production Apps Are Leaking Credentials. The Blindspot DAST Never Checked.

Tags: DEF CON Demo Labs | Intermediate | AppSec | Defense/Blue Team | DevOps | Offense/Red Team | Threat Intel/Hunting | DEF CON Demo Labs

When: Saturday, Aug 8, 10:00 - 10:45 PDT

Where: LVCCW Level 1 Hall 3 1001 (Demo Labs Track 1) - [Map](#)

Description:

Shift-left tools scan what you commit, not what you serve. DAST scanners test for vulnerabilities but ignore live traffic. The industry left a gap: runtime secrets. Finding them requires intercepting live traffic: a proxy, a browser extension, or a bulk scanner. SecretSifter is all three.

We tested 2,000 production apps against ten secret scanners. 194 confirmed credentials survived all ten scanners.

SecretSifter monitors live HTTP traffic and finds credentials in JS bundles, lazy-loaded chunks, HTML responses, JSON and XML APIs, and request headers. No config, no source code. 160+ rules cover vendor tokens (AWS, Azure, Stripe, Twilio, GitHub), entropy-gated patterns, and CryptoJS-encrypted configs where the decryption key is hardcoded in the same bundle. No other scanner catches that case. Bulk mode scans 30-50 targets: paste URLs, scan, optional AI triage, export HTML, CSV, or ZIP.

The session opens with a live tool comparison. Most tools scan one URL at a time and require manual browsing. SecretSifter bulk-scans both targets in parallel. Two findings none of the ten caught: Azure AD credentials baked into a webpack bundle past GitLeaks. A CryptoJS config with the decryption key three lines away.

Your entire pipeline reported green. Were they right? Attendees leave with a free tool to run the same day.

SpeakerBio: Hemanth Gorijala

Hemanth Gorijala is Global Pentest Lead at a Fortune 100 financial services company. He built SecretSifter to close the runtime security gap: the space between where shift-left secret scanning stops and where secrets actually appear in production. His research identified 194 confirmed credentials across 2,000 production applications that bypassed ten secret scanners. He is presenting that research at security conferences across the US. The GT-194 benchmark is published on Zenodo (DOI 10.5281/zenodo.19464446). SecretSifter is open source at github.com/secretsifter.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Nix Vegas Community - Saturday - 14:45-15:15 PDT

Title: Securing Nix Builds using microVMs

Tags: Nix Vegas Community | Creator Talk/Panel

When: Saturday, Aug 8, 14:45 - 15:15 PDT

Where: LVCCW Level 1 Hall 4 1310 (Nix Vegas Community) - [Map](#)

Description:

Recent vulnerabilities like Copy Fail and DirtyFrag have made abundantly clear just how risky it is to run untrusted Nix builds inside your core infrastructure. In response, we at Determinate Systems have begun building every Nix package inside of ephemeral microVMs. This talk covers what microVMs are, how they limit kernel-level vulnerabilities, and how we hope to substantially improve our security posture using this technology.

SpeakerBio: Tristan Ross

I work on supply chain security at Determinate Systems.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Securing the AI Stack and Hunting Across Clouds

Tags: Cloud Village | Creator Event/Activity | Strategic Defense

When: Saturday, Aug 8, 16:00 - 16:59 PDT

Where: LVCCW Level 3 W311 (Cloud Village Labs) B - [Map](#)

Description:

Teams are deploying AI agents fast, often without guardrails. Attackers are exploiting cross-cloud trust to pivot between environments. This lab tackles both.

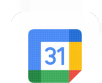
Part A (30 min): Securing the AI Stack- Find over-broad permissions on an AI agent's execution role - Discover prompt injection evidence in model invocation logs - Review Amazon Bedrock Guardrails that block injection, prevent system prompt leakage, and filter PII

Part B (30 min): Cross-Cloud Threat Hunting with OCSF- See how AWS, Azure, and GCP logs map to the same OCSF schema - Trace lateral movement across three clouds using federated identity - Write a detection rule that catches cross-cloud federation abuse

SpeakerBio: Bryant Pickford

Bryant Pickford is a Security Specialist Solutions Architect at AWS, where he leads security, risk, and compliance discussions with enterprise customers to align strategies and drive secure outcomes on the AWS platform. With over five years at AWS and deep expertise in Edge Security, Threat Detection, and Generative AI, Bryant specializes in identifying emerging threats and developing practical defense strategies for cloud-native environments.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

DEF CON Training - Tuesday - 08:30-17:30 PDT

Title: Securing the Future: Defending Kubernetes & Cloud-Native Infrastructure in the Age of AI

Tags: DEF CON Training (Paid) (2-day) | DEF CON Training

When: Tuesday, Aug 11, 08:30 - 17:30 PDT

Where: LVCCW Level 2 W209 (Diana Initiative) - [Map](#)

Description:

SpeakerBio: Madhu Akula

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

DEF CON Training - Monday - 08:30-17:30 PDT

Title: Securing the Future: Defending Kubernetes & Cloud-Native Infrastructure in the Age of AI

Tags: DEF CON Training (Paid) (2-day) | DEF CON Training

When: Monday, Aug 10, 08:30 - 17:30 PDT

Where: LVCCW Level 2 W209 (Diana Initiative) - [Map](#)

Description:

SpeakerBio: Madhu Akula

No BIO available



[Return to Index](#) - Add to Google

- ics [Calendar](#) file

Title: Securing the Safety Net: Why Healthcare Cybersecurity Policy Keeps Failing Patients

Tags: Policy @ DEF CON | Creator Talk/Panel

When: Saturday, Aug 8, 16:00 - 16:59 PDT

Where: LVCCW Level 2 W210-211 (Policy Village) - [Map](#)

Description:

In 2024, ransomware at Change Healthcare didn't just hit one company—it jammed up claims and eligibility checks across the country, squeezed provider cash flow, and made something painfully clear: you can't regulate your way to security when the business model starves defenders of time, staff, and budget. This panel brings two hospital CISOs, a medical device manufacturer's head of product security, and a healthcare policy advocate to talk about the failures that today's policy stack—the HIPAA Security Rule overhaul, HHS Cybersecurity Performance Goals, and proposed CMS conditions of participation—still won't fix. We'll unpack the reimbursement trap (thin margins underinvestment incidents thinner margins unfunded mandates), why devices with decade-long lifecycles end up living forever in clinical environments, and how vendor concentration turns “third-party risk” into systemic risk. This won't be four people nodding. Each panelist will put one concrete intervention on the table—reimbursement-linked incentives, meaningful safe-harbor protections, and supply-chain transparency requirements—then we'll pressure-test the tradeoffs. If you want to understand why healthcare keeps getting owned despite “critical infrastructure” status, and what policy could change the incentive landscape, come argue with us.

Speakers: Sahan Fernando, James Bowie, Nancy Brainerd, Phil Englert

SpeakerBio: Sahan Fernando, Rady Children's Health

Sahan Fernando is the Chief Information Security Officer for Rady Children's Hospital San Diego, one of the nation's top pediatric health care systems. His experience includes security operations and engineering, incident response, and IT and Information Security Program Development in different verticals. He has spoken at multiple security conferences including Cyphercon, SO-CON, Bsides CLT, Health-ISAC, Blue Team Con, and Epic XGM/XGM. He also serves on the board for Health-ISAC.

SpeakerBio: James Bowie, Tampa General Hospital

Jim Bowie is Vice President and Chief Information Security Officer (CISO) at Florida Health Science Center, Inc., responsible for cybersecurity strategy, risk management, and operational defense across FHSC and its affiliated entities. Prior to joining FHSC, he served as Director of Cyber Operations at Moffitt Cancer Center. He has also held multiple roles at Tampa General, including Director of Infrastructure, Cyber Operations, and Clinical Applications Manager, bringing deep experience across clinical technology, operations, and security. Bowie previously worked in law enforcement with the Tampa Police Department, supporting cybersecurity and digital forensics investigations. He began his career in emergency medical services, including service as Director of Emory Emergency Medical Services, a volunteer EMS agency. Bowie earned a master's degree in Cybersecurity and Information Assurance and is currently pursuing a PhD in Cyber Defense along with a second master's degree in Artificial Intelligence. He also holds a BA in History. He is accredited by the College of Healthcare Information Management Executives (CHIME) as a Certified Healthcare Information Security Leader (CHISL) and maintains several additional industry certifications.

SpeakerBio: Nancy Brainerd, Medtronic

Nancy Brainerd joined Medtronic in 2000 kicking off a career in Information Technology. In 2006, she began working within the information security field and had the opportunity to build out Medtronic's first Cyber Defense organization, specializing in cybersecurity incident response. As scrutiny of cybersecurity of medical devices has increased, Nancy made the shift in 2023 to focus on security of Medtronic's products. She is currently a Senior Director in the Product Security Office with

oversight of cybersecurity of Medtronic devices and products. Nancy is active in the security industry and participates in many coordinated activities, including a current directorship on the board for Health-ISAC (Health Information Sharing and Analysis Center). She is a frequent guest lecturer at the University of Minnesota on the topic of Cybersecurity in the “Introduction to Information Technology in Business” undergraduate course.

SpeakerBio: Phil Englert, Health-ISAC

Phil Englert is the VP of Medical Device Security at Health ISAC, where he works with medical device manufacturers to strengthen privacy and security while partnering with healthcare delivery organizations to ensure those solutions are practical, deployable, and clinically aligned. He also defines long term vision, leads cross sector initiatives, advances best practices, and delivers programs that improve sector resilience and serves as a subject matter expert and contributor to Health ISAC’s Medical Device Security Council (MDSC). Phil leads Health ISAC’s strategy to strengthen cybersecurity and privacy across the global medical technology ecosystem. This role directs the organization’s medical device security program, partnering with manufacturers and healthcare delivery organizations to drive practical, secure implementations while shaping regulatory and standards. Phil oversees coordinated vulnerability disclosure efforts with researchers, regulators, and government agencies, and serves as a subject matter expert to the 500 member Medical Device Security Council.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Security Analysis of Open-Source Software Used in Onboard Satellite Systems

Tags: Aerospace Village | Creator Talk/Panel

When: Saturday, Aug 8, 11:00 - 11:30 PDT

Where: LVCCW Level 1 Hall 3 1103 (Creator Stage 5) - [Map](#)

Description:

Satellite missions are increasingly making use of open-source software, but this creates a unique security challenge for space systems. Unlike conventional IT environments, updating software onboard satellites can be far more difficult due to operational risk, limited access windows, mission validation requirements, and the high cost of mistakes after launch. In many cases, space systems also remain in operation for years, which means software may continue running on aging hardware and in environments where patching, upgrading, or fixing security issues is far more constrained than on the ground. This talk presents SCA-SAT, a purpose-built pipeline created to analyze the current security state of open-source software used in onboard satellite systems at scale. The goal is to answer a simple but important question: what does the current security landscape of open-source onboard satellite software actually look like?

SpeakerBio: Roei Idan

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Voting Village - Friday - 16:00-16:30 PDT

Title: Security and Privacy for the Rest of Elections

Tags: Voting Village | Creator Talk/Panel

When: Friday, Aug 7, 16:00 - 16:30 PDT

Where: LVCCW Level 2 W220 (Voting Village) (Voting Village Talks) - [Map](#)

Description:

SpeakerBio: Michael Specter

Michael A. Specter is an Assistant Professor in Computer Science at Georgia Tech where he leads the SPDR Lab. Specter's interests are broadly on problems in systems security and applied cryptography, specifically on issues relevant to public policy. He joined Google after completing his PhD in Electrical Engineering and Computer Science at MIT, and previously served as research staff at MIT's Lincoln Laboratory. His research has been featured in congressional testimony, amicus briefs to the Supreme Court, and (repeatedly) in the popular press. He holds the 2023 Research Award from the Elections Verification Network and a Pioneer Award from the Electronic Frontier Foundation (EFF).

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Security at Machine Speed: How Autonomous AI Agents Are Changing Cloud Defense

Tags: Cloud Village | Creator Talk/Panel

When: Friday, Aug 7, 12:10 - 12:50 PDT

Where: LVCCW Level 3 W313 (Cloud Village Talks) - [Map](#)

Description:

Attackers are using frontier AI to compress the time between finding a vulnerability and exploiting it. Manual triage and human-in-the-loop remediation cannot keep pace. The answer is autonomous security that works at machine speed.

This talk covers the continuous AI-powered security loop and how autonomous agents are changing three SOC functions:

Autonomous triage. Agentic AI systems trained on real security decisions separate real threats from noise with high accuracy, reasoning across logs, configurations, reachability, and history. What takes analysts hours, these systems handle in seconds.

Validated remediation. The latest AWS security enhancements discover vulnerabilities, validate exploitability in sandboxes, and fix confirmed exposures with increasing autonomy. We walk through the journey from human-approved fixes to fully autonomous remediation.

Continuous offensive testing. AI agents that proactively test your applications throughout the dev lifecycle instead of once a year. Customized pen testing across your whole environment. We show what this looks like when an AI chains attack paths across services in real time.

The full loop. Discovery feeds triage, triage feeds remediation, remediation closes the gap before attackers exploit it. Integrated through AWS Security Hub with the tools you already use.

Real demos. Real attack paths. Walk away knowing where this technology stands and what first steps look like.

Speakers: Pujita Sahni, Geoff Sweet

SpeakerBio: Pujita Sahni

Pujita Sahni is a Delivery Consultant specializing in cloud security, risk, and compliance at AWS. In her role, she is responsible for architecting IAM governance frameworks and security automation solutions that enable organizations to implement secure cloud migrations and shift security left within enterprise environments. She brings a broad technical background across identity and access management, vulnerability management, infrastructure-as-code security, and DevSecOps practices, providing a comprehensive view of how security platforms are built, automated, and maintained across enterprise cloud environments.

SpeakerBio: Geoff Sweet

Geoff Sweet has nearly 30 years of technology experience, starting from the late 90's during the dot-com boom. Geoff has worked in many verticals including Gaming, BioTech, Retail, and financial SaaS. He has held several titles through his career such as Systems Architect, Network Architect, and most recently Security Architect. These experiences have helped him to develop robust experiences in Infrastructure Security. Geoff left the customer side to come to AWS in December of 2019. He left SAP where he lead a small security team responsible for monitoring and doing Incident Response for nearly 10,000 cloud accounts over several cloud providers. Geoff has a proven record of speaking to customers in both small and large format settings. He is engaging, entertaining, and communicates in a way that assures everyone understands. Geoff's background is in Electrical Engineering and Mathematics and continues to use that knowledge to support his customers. He also has a deep fondness for all things automotive and extensive experience building and fabricating vintage cars.



Radio Frequency Village - Friday - 14:30-14:55 PDT

Title: Security Vulnerabilities in SATCOM Devices

Tags: Radio Frequency Village | Creator Talk/Panel

When: Friday, Aug 7, 14:30 - 14:55 PDT

Where: LVCCW Level 1 Hall 1 409 (Radio Frequency Village) - [Map](#)

Description:

This presentation delivers a deep-dive security analysis of satellite communication (SATCOM) systems, bridging the gap between theoretical vulnerabilities and hands-on, non-intrusive experimental observation. By examining representative broadband terminals and Low Earth Orbit (LEO) satellite phone systems, we dissect how architectural and implementation choices create distinct security risks across firmware, management interfaces, and radio-frequency (RF) communication layers. Using commodity Software-Defined Radio (SDR) hardware and open-source tools, we successfully executed passive RF observation experiments to characterize Iridium L-band downlink activity. The highlight of this session is the demonstration of an end-to-end pipeline that captured and reconstructed satellite voice transmissions, including emergency traffic, directly from the air.

SpeakerBio: Aumkareshwar DS

I am a Computer Science graduate student at California State Polytechnic University, Pomona, passionate about cybersecurity, network security, and ethical hacking. Currently, I work as a Research Assistant at PolySec Lab, where I focus on 5G network security, including authentication, subscriber identity protection, and threat mitigation. My research helps enhance mobile security and protect data from cyber threats.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Self Hosting Nightmare - Exploiting AI models for supply chain attacks

Tags: La Villa Community | Creator Talk/Panel

When: Saturday, Aug 8, 10:30 - 10:59 PDT

Where: LVCCW Level 1 Hall 4 1416 (La Villa Community) Main Stage - [Map](#)

Description:

In this presentation I'll go through the process of how you could possibly exploit this vulnerability in one of thousands servers exposed to the internet running the top one tool in the world for self hosting AI models. The process I'll demonstrate in this presentation involves exploring vulnerable by default decisions to achieve total control of this model serving tool, and the vulnerability research I have done on top of this tool that led me to find 7 0day vulnerabilities that allows anyone to achieve the following results:

- Free token usage
- Cause unavailability in the servers
- Steal top of the market secret models
- Cause chaos within dependent services with a model defacement
- Craft a supply attack

SpeakerBio: Davidson Mizael, Incident Responder @ IBM X-Force

Long time hacker and former developer working at IBM X-Force doing Incident Response.

Hacking for the fun of it and always trying to building cool stuff.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: SEND: Teaching Machines to Lie to Defenders

Tags: Adversary Village | Creator Talk/Panel

When: Friday, Aug 7, 14:45 - 15:15 PDT

Where: LVCCW Level 1 Hall 3 1105 (Creator Stage 3) - [Map](#)

Description:

Cyber deception research has spent decades placing honeypots, honeyfiles, and fake credentials in enterprise environments to catch attackers. Yet practitioners in real Security Operations Centers do not investigate individual artifacts in isolation — they construct causal narratives to explain sequences of events, routing attention toward high-severity signals, end-of-attack-chain activities, and operations in sensitive infrastructure. As Sundaramurthy et al. documented through ethnographic study of live SOC environments, analyst behavior under alert overload is governed by triage heuristics and pattern-matching rather than systematic evidence review — creating a systematic cognitive attack surface that no existing offensive framework has been designed to exploit.

In this work, we introduce SEND (Self-Evolving Narrative Deception), an adversary simulation framework that reframes offensive deception as an investigation narrative poisoning problem: the objective is not to evade detection, but to corrupt the causal story defenders reconstruct during incident response. Drawing on direct consultation with active SOC analysts and incident responders, we identify three empirically grounded cognitive attack vectors that structure the SEND action space — (a.) severity escalation exploitation, targeting the operational requirement to fully investigate HIGH/CRITICAL alerts regardless of underlying harm, (b.) end-of-chain activity simulation, targeting mandatory runbook escalation triggered by ransomware staging or exfiltration patterns regardless of actual file content, and (c.) sensitive location poisoning, targeting the elevated investigative attention guaranteed by activity near domain controllers, privileged shares, and executive endpoints.

We present a design analysis showing that each attack vector can be instantiated at negligible red team cost — failed LSASS reads, dummy outbound transfers of random bytes, and mass-created ransomware-extension files are designed to generate the same mandatory investigation burden as their genuine counterparts, without requiring those actions to succeed. A key design distinction structures the SEND action space: activity simulation generates authentic system telemetry that defenders cannot distinguish from genuine attacker behavior at the telemetry level, while artifact implantation provides cross-system narrative coherence. A Narrative Consistency Engine coordinates both modalities using an LLM to ensure every fabricated email thread, file access log, and collaboration platform entry supports a single coherent false story — shifting the defender's task from "did something anomalous happen?" to "which of several plausible explanations is true?" Moreover, to enable rigorous evaluation of narrative deception beyond detection evasion metrics, we introduce the Investigation Narrative Divergence Reward (INDR) — a four-dimensional cognitive metric quantifying divergence across event reconstruction, causal graph structure, inferred attacker intent, and attribution outcome. INDR is designed to capture a class of deception success that existing red team metrics cannot measure: a defender may correctly identify every process in a malicious process tree yet still produce an incident report attributing the wrong objective, wrong actor, and wrong scope. We further formalize Investigation Graph Poisoning as a measurable attack surface, and outline experimental protocols for evaluating SEND across SOC environments of varying maturity, tooling, and analyst expertise.

In conclusion, SEND establishes the incident investigation itself as a first-class attack surface in adversary simulation, derives deception strategy from empirically grounded blue team cognitive prioritization rather than intuition, and proposes INDR as a new evaluation metric for simulation fidelity — one that asks not whether a simulation triggered alerts, but whether it distorted the reasoning of the defenders who responded to them. Our framework operationalizes at a systematic level what nation-state actors have long practiced intuitively, and makes that threat model legible enough for both red teams and defenders to reason about and build against.

Speakers: Yi Ting Shen, Ariz Soriano

SpeakerBio: Yi Ting Shen, AIFT - Associate GenAI Security Researcher

I am currently working as a Associate Associate GenAI Security Researcher at AIFT. Over the past year, I have presented various cybersecurity-related research topics at more than 20 domestic and international conferences (DEFCON, ROOTCON, BSides..). I enjoy conducting research, especially focusing on AI/ML applications this year. By engaging with different technical domains, I aim to solve cybersecurity problems, uncover vulnerabilities across various platforms, and identify new CVE vulnerabilities. I have found vulnerabilities in multiple platforms, including Google, Cloudflare, open-source projects, and educational institutions. Learning and research have become the central focus of my life.

Blog: <https://no-flag.com/>

SpeakerBio: Ariz Soriano, Associate Director - Red Team Operations @ THEOS Cyber Solutions

Ariz Soriano is Associate Director of Red Team at Theos, with nearly a decade of experience spanning Red Teaming, Penetration Testing, and Incident Response. He started his career on the defensive side, working as a SOC analyst and eventually leading SOC and IR teams for his first four years in the industry. That defensive foundation gives him a perspective most purely offensive operators don't have.

He built the Theos Red Team from the ground up, recruiting and training operators, designing red team infrastructure and tooling, and establishing the methodology and playbooks behind the team's APT simulation and purple teaming engagements. Today he runs a practice that delivers multiple concurrent engagements a year, balancing operations with presales, scoping, revenue targets, and people management.

Outside of client work, Ariz is passionate about building red team tooling, optimizing offensive workflows, and sharing knowledge with the community as a conference speaker. He also contributes to TryHackMe as a part-time Senior Content Engineer, creating hands-on cybersecurity labs and challenges based on real-world attack techniques.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Senrigan () x Suzaku (): Threat Hunting & DFIR for AWS — No SIEM, Just Your Laptop

Tags: DEF CON Demo Labs | Intermediate | Cloud | Defense/Blue Team | Purple Team | Threat Intel/Hunting | DEF CON Demo Labs

When: Saturday, Aug 8, 14:00 - 14:45 PDT

Where: LVCCW Level 1 Hall 3 1003 (Demo Labs Track 3) - [Map](#)

Description:

Senrigan () and Suzaku () are two complementary open-source tools that together form a complete threat hunting and DFIR platform for AWS CloudTrail logs. Both are built by Yamato Security, the volunteer-run Japanese security community behind Hayabusa°, Ì , the widely adopted Windows event log fast-forensics tool. Yamato Security provides free, open-source DFIR tools and resources to the community.

Building on Hayabusa's philosophy of fast, offline, community rule-based detection, this toolset brings the same approach to the cloud. Security teams can hunt threats across CloudTrail logs on a single laptop — without a SIEM, dedicated infrastructure, or licensing cost.

The two tools work together, with Suzaku's detections flowing into Senrigan for analysis. Senrigan, deployed via Docker Compose, ingests CloudTrail logs into DuckDB via a Rust-based ingester, then lets analysts investigate them through 100+ pre-built hunting queries and 80+ pre-built Apache Superset dashboard charts — no SQL or CloudTrail schema knowledge required. Suzaku is a high-performance, standalone Rust-based CLI that applies native Sigma detection rules to CloudTrail logs and generates a fast-forensics DFIR timeline — surfacing attacks buried in the noise, producing only the events analysts need to investigate.

Speakers: Fukusuke Takahashi, Zach Mathis, Akira Nishikawa

SpeakerBio: Fukusuke Takahashi

Fukusuke Takahashi has been with NTTDATA-CERT (NTT DATA Group Corporation's CSIRT) since 2018, specializing in DFIR, OSINT, and SOAR. He is one of the developers of Yamato Security's OSS tools. He enjoys developing open-source Blue Team tools. He has presented at conferences such as FIRST Annual Conferences, SECCON, BSides Tokyo, HITCON CMT, SecTor and AUSCERT.

SpeakerBio: Zach Mathis

Zach Mathis has been working in Japan doing offensive and defensive security work for Japanese companies since 2006. In 2012, he founded Yamato Security, one of the largest hands-on hacker communities in Japan. With other Yamato Security members, he has been releasing free and open source DFIR tools and resources since 2020.

SpeakerBio: Akira Nishikawa

Akira Nishikawa started his career as a software engineer specializing in embedded development. He worked as a freelance engineer in 2007, focusing on system development and operation for various companies. Since 2021, he has been dedicated to fostering a security culture for SaaS product security and improving service security. Additionally, he is an AWS Community Builder as of 2024.





Title: Senrigan () x Suzaku (): Threat Hunting & DFIR for AWS — No SIEM, Just Your Laptop

Tags: DEF CON Demo Labs | Intermediate | Cloud | Defense/Blue Team | Purple Team | Threat Intel/Hunting | DEF CON Demo Labs

When: Friday, Aug 7, 10:00 - 10:45 PDT

Where: LVCCW Level 1 Hall 3 1003 (Demo Labs Track 3) - [Map](#)

Description:

Senrigan () and Suzaku () are two complementary open-source tools that together form a complete threat hunting and DFIR platform for AWS CloudTrail logs. Both are built by Yamato Security, the volunteer-run Japanese security community behind Hayabusa°, the widely adopted Windows event log fast-forensics tool. Yamato Security provides free, open-source DFIR tools and resources to the community.

Building on Hayabusa's philosophy of fast, offline, community rule-based detection, this toolset brings the same approach to the cloud. Security teams can hunt threats across CloudTrail logs on a single laptop — without a SIEM, dedicated infrastructure, or licensing cost.

The two tools work together, with Suzaku's detections flowing into Senrigan for analysis. Senrigan, deployed via Docker Compose, ingests CloudTrail logs into DuckDB via a Rust-based ingester, then lets analysts investigate them through 100+ pre-built hunting queries and 80+ pre-built Apache Superset dashboard charts — no SQL or CloudTrail schema knowledge required. Suzaku is a high-performance, standalone Rust-based CLI that applies native Sigma detection rules to CloudTrail logs and generates a fast-forensics DFIR timeline — surfacing attacks buried in the noise, producing only the events analysts need to investigate.

Speakers: Fukusuke Takahashi, Zach Mathis, Akira Nishikawa

SpeakerBio: Fukusuke Takahashi

Fukusuke Takahashi has been with NTTDATA-CERT (NTT DATA Group Corporation's CSIRT) since 2018, specializing in DFIR, OSINT, and SOAR. He is one of the developers of Yamato Security's OSS tools. He enjoys developing open-source Blue Team tools. He has presented at conferences such as FIRST Annual Conferences, SECCON, BSides Tokyo, HITCON CMT, SecTor and AUSCERT.

SpeakerBio: Zach Mathis

Zach Mathis has been working in Japan doing offensive and defensive security work for Japanese companies since 2006. In 2012, he founded Yamato Security, one of the largest hands-on hacker communities in Japan. With other Yamato Security members, he has been releasing free and open source DFIR tools and resources since 2020.

SpeakerBio: Akira Nishikawa

Akira Nishikawa started his career as a software engineer specializing in embedded development. He worked as a freelance engineer in 2007, focusing on system development and operation for various companies. Since 2021, he has been dedicated to fostering a security culture for SaaS product security and improving service security. Additionally, he is an AWS Community Builder as of 2024.





Title: Separating News from Noise

Tags: Voting Village | Creator Talk/Panel

When: Saturday, Aug 8, 14:00 - 14:30 PDT

Where: LVCCW Level 2 W220 (Voting Village) (Voting Village Talks) - [Map](#)

Description:

News versus noise. Every election cycle brings a flood of headlines covering changes to election administration, election security, and the voter experience. The 2026 midterm elections will unfold amid significant legal, policy, and election security developments. What developments will have the most impact on the 2026 midterm elections and beyond, and which are unlikely to have a lasting impact? Join a panel of election administrators, legal experts, and cybersecurity professionals as they analyze the year's most significant election developments, separate consequential changes from background noise, and discuss their practical implications for election administration, cybersecurity, and the voter experience. Topics include federal and state election laws, executive orders, SCOTUS rulings, redistricting disputes, election security, and other issues influencing both the immediate and long-term future of American elections. Attendees will leave better equipped to distinguish consequential election developments from background noise and understand how those developments affect election administration, cybersecurity, voter confidence, and the voter experience.

Speakers: Ryan Murray, Stephen Richter, Nate Young

SpeakerBio: Ryan Murray

Ryan Murray is Deputy Director and CISO of Arizona DHS. He has his finger on the pulse of current elections cybersecurity operations from the AZ-ISAC (Information and Analysis Center) and AZ-DHS (Dept. of Homeland Security) fusion center operations.

SpeakerBio: Stephen Richter

Stephen Richer is a legal fellow with the Cato Institute's Robert A. Levy Center for Constitutional Studies. His work focuses on election administration, American democracy, executive orders, and American politics. He is a visiting senior fellow at the Ash Center for Democratic Governance and Innovation at Harvard University's Kennedy School. He is also the CEO of Republic Affairs, a crisis consulting firm for pro-democracy, pro-rule-of-law entities and individuals. He was the Maricopa Recorder from 2021 - 2025, and experienced first hand the Arizona Senate Audit (CyberNinjas) and related Department of Justice Investigations.

SpeakerBio: Nate Young

Nate Young is the Deputy CIO of Elections Information Technology for Maricopa County, where he leads a dedicated team of career IT professionals focused on supporting and facilitating secure, accurate, and accessible elections. With 19 years of experience across government and the education sector, Nate brings a broad and practical perspective to public-sector technology. Since 2021, Nate has focused on elections technology and cyber security since 2021 with the 2020 Elections audit from the Cyber Ninjas. Nate has presented at many Elections and cyber security related conferences, including the DEFCON Voting Village 2022, 2024, 2025.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: SH4ZAM: Accelerated Vector Math on the Sega Dreamcast

Tags: Game Hacking Village | Creator Talk/Panel

When: Sunday, Aug 9, 12:30 - 12:59 PDT

Where: LVCCW Level 1 Hall 3 801 (Creator Stage 2) - [Map](#)

Description:

SH4ZAM is a hardware accelerated, fast math and linear algebra library targeting the Sega Dreamcast. It began as a collection of hand-optimized SH4 assembly routines I wrote to boost the performance of our "impossible" ports of Grand Theft Auto 3 and Vice City to the DC. It has since evolved into a standalone library, offering a full, optimized math solution to the Sega Dreamcast homebrew community at large, accelerating the performance behind many of the community's other high-profile ports (Super Mario 64, Mario Kart 64, Star Fox 64, and now Zelda: Ocarina of Time) as well as original homebrew games, apps, and engines.

Despite targeting a game console that is over 25 years old now, the library is written to be especially cutting-edge, targeting the latest GCC 15.2 toolchains and providing dual, modern C23 and C++23 APIs. Additionally, it now features a generic software back-end, which allows for the library to be built for any non-Dreamcast target, facilitating easily porting SH4ZAM'd code or utilizing it in cross-platform codebases. The software back-end has already enabled the community to re-port our Dreamcast port of Super Mario 64 to the Nintendo Gamecube without having to change a line of math code!

For the talk, I'd like to cover an array of topics, touching on the specific hardware features of the Dreamcast's FPU that SH4ZAM is exploiting via SH4 assembly, high-level overviews of the library's architecture and layering of its C and C++ APIs, and providing some general takeaways for modern vectorization libraries, as a lot of this is applicable to many other game consoles or even modern performance-focused mathematics libraries in general.

The talk will also feature a brief introduction to the Sega Dreamcast homebrew scene, explaining why the console remains such an ideal target for indie developers despite its age and including a high-level overview of the tools and SDK we use to develop modern software for it. Finally, the talk will feature many screenshots and embedded video segments of some of these SH4ZAM'd up codebases, including many of our high-profile AAA ports.

SpeakerBio: Falco Girgis

Falco Girgis is a veteran developer in the Sega Dreamcast homebrew scene and a regular contributor to the KallistiOS indie SDK and operating system, where he has worked to bring support for modern C23 and C++23 language standards to the platform. He has been involved in many high-profile ports to the DC, such as Grand Theft Auto 3, Grand Theft Auto: Vice City, Mario Kart 64, Sonic Mania, and more!

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Shadow Webhooks: Hunting for Dangling Event Listeners in Enterprise Workspaces

Tags: Bug Bounty Village | Creator Talk/Panel

When: Saturday, Aug 8, 10:00 - 10:30 PDT

Where: LVCCW Level 1 Hall 3 1102 (Creator Stage 6) - [Map](#)

Description:

Enterprise SaaS environments accumulate webhooks faster than teams can track them. Slack apps, Teams connectors, Jira automations, GitHub webhooks, CI/CD callbacks, monitoring alerts, and abandoned integrations often remain active long after the receiving service, repository, domain, or owner disappears. These forgotten event listeners can become quiet security liabilities: they may leak event payloads, accept forged messages, expose secrets in callback URLs, or create takeover paths when linked infrastructure expires. This talk presents a practical bug bounty methodology for finding and reporting “shadow webhooks”: trusted event connections that still exist inside an enterprise workspace but no longer have a clear owner, valid destination, or reliable validation model. I will cover how to inventory webhook surfaces, classify destination risk, fingerprint abandoned endpoints, identify dangling domains or retired cloud functions, test signing and replay behavior safely, and prove impact without collecting real third-party data. The demo uses a controlled lab that models common workflows across source control, ticketing, chat, and CI/CD systems. One webhook points to a retired destination. Another accepts events without strong signature validation. The audience will see how synthetic project events and incident notifications can reach the wrong endpoint, how weak validation allows forged events, and how the issue should be documented for a bounty program. The talk also covers what makes a webhook finding triageable: affected asset, trusted event source, destination ownership, payload sensitivity, validation weakness, and business impact. For defenders and program owners, it provides controls for webhook inventory, owner mapping, event signing, secret rotation, endpoint expiration, and domain lifecycle monitoring. The goal is to turn forgotten webhook exposure from a vague SaaS hygiene issue into a clear, reproducible bug bounty finding.

Speakers: Samet Can Tasci, Mehmet Önder Key

SpeakerBio: Samet Can Tasci, Senior Linux Systems Engineer

Samet Can Tasci is a Senior Linux Systems Engineer and security researcher with experience across enterprise infrastructure, cloud and hybrid environments, automation, and defensive security validation.

His research interests include web defense behavior, WAF normalization gaps, parser inconsistencies, adversary-informed testing, and practical tooling for security teams.

He is the creator of WaffleX, a research prototype selected for Black Hat USA Arsenal, which focuses on semantic consistency analysis, enforcement drift, and family-level request-variant testing across modern web application defense stacks.

SpeakerBio: Mehmet Önder Key, Cyber Security Consultant

Önder Key is a cybersecurity consultant specializing in critical infrastructure security, zero-day vulnerability analysis, and offensive security. He has advised organizations in high-security sectors such as defense, aerospace, and finance, with hands-on experience in both red teaming and strategic security engineering. His work has been featured across numerous countries and platforms, contributing to the discovery of systemic vulnerabilities. Currently, he provides consultancy to TurkNet and continues to advance the global offensive security ecosystem by challenging traditional approaches to cybersecurity.

Title: Shapeshifting C2: Applying DAITA Traffic Shaping to Defeat DPI and DLP Detection

Tags: Red Team Village | Misc

When: Friday, Aug 7, 13:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 1 309 (Red Team Village) Workshop Stage 1 - [Map](#)

Description:

ML-based DPI and DLP solutions have made signature evasion insufficient. Modern enterprise detection analyzes packet size distributions, inter-packet timing, and burst patterns to fingerprint C2 traffic regardless of how well headers and TLS certificates are spoofed.

This talk demonstrates how three techniques from the VPN privacy research space - originally developed to defeat traffic analysis against Tor and Mullvad, can be adapted for offensive C2 operations:

1. Constant-size packet morphing: forcing all frames to a fixed MTU-aligned size removes the packet-size fingerprint that ML classifiers depend on;
2. Cover traffic injection: dummy packets sent at Poisson-distributed or adaptive intervals make real beacon timing statistically invisible;
3. Probabilistic pattern distortion: Maybenot-inspired state machines inject cover bursts alongside real packets, destroying recognizable C2 sequences;

We then will see how layering these techniques with application-layer malleable profiles (traffic impersonating Microsoft Graph, Slack, or Okta) and bonus: indirect transports like cloud storage dead-drops (S3, OneDrive) creates C2 channels that defeat detection at every layer simultaneously - behavioral, flow, and application.

Attendees leave with a concrete mental model for building evasion stacks that go beyond header manipulation.

SpeakerBio: Rafael Felix, Offensive Security Lead at Hakai Offensive Security

Rafael has been working with malware development for 5 years, also being involved in the malware community for more than 7 years. He is also experienced in Incident and Response, specifically during malware inner workings analysis. Currently, Rafael is a researcher for Hakai Offensive Security (<https://hakaisecurity.io/research-blog>), being deeply involved with red-team operations.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Shepherd the Tor network

Tags: DEF CON Official Talk

When: Sunday, Aug 9, 10:00 - 10:59 PDT

Where: LVCCW Level 1 Hall 3 903 (Main Track 5) - [Map](#)

Description:

The Tor network has been continuously operating for close to 25 years now. How have the attacks changed over that time? How about the communities, threats, and incentive structures for the volunteers who operate the network?

I'll go over early lessons as well as lessons we are still learning, when it comes to the Tor network -- from relays to directory authorities -- focusing on the community angle, on finding and kicking out bad relays, and generally looking at the safety of users and of relay operators.

<https://community.torproject.org/policies/relays/expectations-for-relay-operators/>

https://community.torproject.org/policies/dir-auth/dir_auth_expectations/

<https://www.freehaven.net/anonbib/#botnetfc14>

<https://spec.torproject.org/vanguards-spec/>

<https://research.torproject.org/safetyboard/>

SpeakerBio: Roger "arma" Dingledine, The Tor Project

Roger Dingledine is co-founder and original developer of the Tor Project, a nonprofit that develops free and open source software to protect people from tracking, censorship, and surveillance online. Roger works with journalists and activists on many continents to help them understand and defend against the threats they face, and he is a lead researcher in the online anonymity field. EFF picked him for a Pioneer Award, and Foreign Policy magazine chose him as one of its top 100 global thinkers. This is his twelfth talk on the Defcon main stage.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Maritime Hacking Village - Saturday - 16:00-16:30 PDT

Title: Shipcrawler: Automated Maritime OSINT — From Open Data to Actionable Intelligence

Tags: Maritime Hacking Village | Creator Talk/Panel

When: Saturday, Aug 8, 16:00 - 16:30 PDT

Where: LVCCW Level 1 Hall 3 801 (Creator Stage 2) - [Map](#)

Description:

The maritime sector leaks an enormous amount of sensitive information through public sources — crew social media, vessel tracking data, port records, corporate registries, and leaked credentials. Shipcrawler is an open-source automated OSINT tool that aggregates, correlates, and reports on vessel, crew, company, and port authority intelligence from publicly available sources. Built with a queue-based architecture and AI Agent-powered worker pipeline, it has produced over seven comprehensive intelligence reports covering vessels, port authorities, and maritime personnel. This talk demonstrates OSINT collection against maritime targets, discusses the ethical and operational implications of maritime data exposure, and shows how OSINT audits can inform defensive posture improvements. All code and methodologies are open-source to help the maritime community understand their own attack surface.

SpeakerBio: Ahmed Nagi Nasr, Estonian Maritime Academy - Tallinn University of Technology (TalTech)

Maritime cybersecurity researcher at TalTech, author of Shipcrawler and Project Haris. Published in IEEE Access, TransNav, J. Marine Science. Focused on open-source defense tools for maritime IT/OT security.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Shopping Is The Attack: A Decade Of E-Commerce Scalper Wars, And The Multi-Agent AI Era

Tags: DEF CON Official Talk

When: Friday, Aug 7, 12:00 - 12:30 PDT

Where: LVCCW Level 1 Hall 3 903 (Main Track 5) - [Map](#)

Description:

Forty-five seconds. Two thousand five hundred Nike Air Jordans, gone. Resold at five times retail the next month. Every weekly drop, for years, at one of Europe's largest retailers.

Shopping is the attack. The bot does not exploit a CVE. It does not break the contract. It just shops, and every standard control is structurally blind to it.

I spent five years as Head of SecOps at ASOS, on the bridge for every Air Jordan drop, reverse-engineering the full attacker MO because nobody else was going to.

This talk is that MO from the attacker's chair. Eight phases against the e-commerce golden thread. Account army staged weeks ahead via fake registration and credential stuffing. Targets picked from StockX margins, not catalogues. Early bird APIs leaking pre-release products before the SKU exists. Mobile catalogue enumeration. Vision-API classification. A watcher polling stock until launch. Two bag agents racing, one guest for raw speed, one aged returning customer for trust. Checkout picked for approval probability. Then I show what Anthropic's GTG-1002 disclosure means for retail: the same MO, decomposed into AI agents, at speeds Anthropic called physically impossible.

The eCommerce bots are unstoppable. Come see why.

SpeakerBio: Yaniv "PSYMAG" Menasherov

Yaniv Menasherov has worked every seat in the SOC. He started as a Tier 1 analyst and worked his way up through shift lead, incident response manager, and Head of SOC, the analyst getting paged at 3 AM, the lead running the war room, and the one writing the post-mortem nobody wanted to read.

He's fought them all from both sides of the table: as a client defending enterprises against ransomware crews, insiders, and the occasional state-aligned visitor with too much patience; and as a vendor, sitting next to customers when their existing stack wasn't cutting it. Eventually he founded his own MSSP, building a unified global SOC for some of the largest enterprises in the world, 24/7 across continents, where "alert fatigue" is a polite way of saying "we're losing."

Today he leads research at Legion Security, an agentic SOC platform rethinking investigation and response for a world where analysts shouldn't be the bottleneck. After years of watching SIEMs and SOARs over-promise, he's building what he wished he'd had on shift.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Sick Signals: Adversarial Prompt Injection via Medical IoT Telemetry

Tags: IoT Village | Creator Talk/Panel

When: Friday, Aug 7, 10:45 - 11:30 PDT

Where: LVCCW Level 1 Hall 3 1105 (Creator Stage 3) - [Map](#)

Description:

Medical IoT devices such as continuous glucose monitors, ECG patches, remote patient monitoring hubs that increasingly feed LLM-powered clinical decision systems. Their telemetry streams are implicitly trusted as ground truth. This talk introduces a novel attack class: adversarial prompt injection delivered through crafted medical IoT sensor payloads. By encoding malicious instructions inside what appears to be routine device data, an attacker can manipulate the downstream LLM pipeline, suppressing critical clinical alerts, fabricating findings in physician summaries, or triggering unauthorized actions in AI systems with actuation capabilities. We present the threat model and a taxonomy of seven injection vectors spanning the full stack: analog spoofing, FHIR/HL7 free-text field poisoning, MQTT broker injection, calibration event hijacking, alarm message hijacking, time-series fragmentation, and multi-device coordinated injection. Unlike attacks targeting text interfaces, this class exploits the implicit trust placed in sensor telemetry — payloads hide inside ordinary device data, bypassing numeric validators and arriving in the LLM context as trusted clinical input. We discuss early experimental findings on the feasibility of this attack class, along with detection strategies and open questions for defenders. Attendees will leave with a concrete threat model, an expanded vocabulary for this new attack surface, and a new way to think about trust boundaries in AI-augmented medical systems.

Speakers: Vinitha Mathiyazhagan, Tamil Mathi T.

SpeakerBio: Vinitha Mathiyazhagan

No BIO available

SpeakerBio: Tamil Mathi T.

No BIO available

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Telecom Village - Saturday - 14:00-14:15 PDT

Title: Signal Hijacked: How Mobile Networks Became Phishing's Most Trusted Delivery Layer

Tags: Telecom Village | Creator Talk/Panel

When: Saturday, Aug 8, 14:00 - 14:15 PDT

Where: LVCCW Level 3 W321 (Telecom Village) - [Map](#)

Description:

1. Live Demonstration: "The Signal Switch"
2. Display a realistic QR code (restaurant menu, airport Wi-Fi, or bank notification).
3. Ask the audience whether they would scan it.
4. Walk through what happens after scanning.
5. Show how the phishing page is delivered over a trusted mobile channel (WhatsApp/SMS simulation).
6. Demonstrate analytics showing user interactions and explain how attackers track victims.
7. Compare the same QR code against AI analysis (ChatGPT, Claude, Gemini) and highlight the differences in detection.

SpeakerBio: Sindhura Kona

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Telecom Village - Saturday - 12:30-12:59 PDT

Title: Signaling Sabotage: Why 100% Compliance is 0% Security

Tags: Telecom Village | Creator Talk/Panel

When: Saturday, Aug 8, 12:30 - 12:59 PDT

Where: LVCCW Level 3 W321 (Telecom Village) - [Map](#)

Description:

Why 100% Compliance is 0% Security exposes the dangerous false sense of security that compliance audits create in modern telecommunications. While regulatory checklists establish a baseline, real-world threat actors routinely bypass compliant controls to exploit critical protocol vulnerabilities across SS7, Diameter, GTP, and SIP networks. This talk bridges the gap between regulatory requirements and real-world operational security, highlighting live-fire signaling attack techniques and hidden abuse cases that traditional audits miss. Attendees will learn why standard compliance falls short and discover actionable strategies for building true resilience—leveraging proactive threat hunting, offensive security

SpeakerBio: Vinod Shrimali

No BIO available

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Telecom Village - Friday - 15:00-15:30 PDT

Title: SIM Card Strikes Back: Telecom Threats & SOC Detection

Tags: Telecom Village | Creator Talk/Panel

When: Friday, Aug 7, 15:00 - 15:30 PDT

Where: LVCCW Level 3 W321 (Telecom Village) - [Map](#)

Description:

What will be covered:

1. Understanding the SIM Attack Surface – Why SIM cards are a critical part of the tele-com security ecosystem.
2. Common Telecom Threats – SIM Swap, SS7 abuse, IMSI Catchers, SMS OTP bypass, and insider threats.
3. SOC Detection Strategies – Identifying suspicious SIM, subscriber, and signaling active-ties using effective monitoring techniques.
4. Threat Correlation – Connecting telecom events with identity and security logs for faster incident detection and response.
5. Strengthening Telecom Security – Best practices to improve SOC visibility and reduce risks associated with SIM-based attacks.

SpeakerBio: Zibran Sayyed

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

DEF CON Training - Tuesday - 08:30-17:30 PDT

Title: Simulated Adversary: Tactics & Tools Training

Tags: DEF CON Training (Paid) (2-day) | DEF CON Training

When: Tuesday, Aug 11, 08:30 - 17:30 PDT

Where: LVCCW Level 2 W205 (Payment Village) - [Map](#)

Description:

Speakers: Jayson E. Street, Iain Jackson, James Sheppard

SpeakerBio: Jayson E. Street, CovertSwarm

No BIO available

SpeakerBio: Iain Jackson, CovertSwarm

No BIO available

SpeakerBio: James Sheppard, CovertSwarm

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

DEF CON Training - Monday - 08:30-17:30 PDT

Title: Simulated Adversary: Tactics & Tools Training

Tags: DEF CON Training (Paid) (2-day) | DEF CON Training

When: Monday, Aug 10, 08:30 - 17:30 PDT

Where: LVCCW Level 2 W205 (Payment Village) - [Map](#)

Description:

Speakers: Jayson E. Street, Iain Jackson, James Sheppard

SpeakerBio: Jayson E. Street, CovertSwarm

No BIO available

SpeakerBio: Iain Jackson, CovertSwarm

No BIO available

SpeakerBio: James Sheppard, CovertSwarm

No BIO available



[Return to Index](#) - Add to Google

- ics [Calendar](#) file

Title: sisakulint:CI-Friendly static linter with autofix, SAST, semantic analysis for GitHub Actions

Tags: AI | DEF CON Demo Labs | Intermediate | AppSec | Cloud | DevOps | Purple Team | DEF CON Demo Labs

When: Friday, Aug 7, 11:00 - 11:45 PDT

Where: LVCCW Level 1 Hall 3 1002 (Demo Labs Track 2) - [Map](#)

Description:

GitHub Actions workflows are vulnerable by default. Hardening such as commit-hash pinning, least-privilege permissions, and timeouts is optional, never enforced at pipeline level. Exploitable configs ship daily, increasingly written by Coding Agents. sisakulint is a fast heuristic static analyzer for GitHub Actions covering all OWASP Top 10 CI/CD risks, with 52 rules, a taint engine, and 38+ auto-fixes. It outpaces CodeQL on speed and quality, with 100% detection on 18 GHSL advisories and 81.6% on 38 GHSAs covering exploits in PX4-Autopilot, vets-api, weaviate, nrwl/nx.

Impostor Commit at CVSS 9.8 validates pinned SHAs against the claimed repository, not impostors via Git forks, a check unique to sisakulint. Code Injection at CVSS 9.8 tracks untrusted input through ``${}`` and step outputs. AI Action Rules detect Clinejection on claude-code-action, copilot-swe-agent, and openai-actions, covering tool grants, prompt injection, and wildcard triggers, as in Cline 2026/02 where issue title injection stole NPM_RELEASE_TOKEN. Known Vulnerable Actions catches tj-actions/changed-files.

In the Coding Agent era, linters matter more. Delegating 52 rules to an LLM degrades precision; deterministic engines run in ms with no variance. The session covers end-to-end detection, taint propagation, and automated remediation.

Speakers: Atsushi Sada, hikae

SpeakerBio: Atsushi Sada

Atsushi Sada is a CSIRT member specializing in cloud security on AWS and GitHub, and enterprise security with MDM, EDR, AI governance. He is an ethical hacker and security tool developer. He built sisakulint and MachStealer for practical security research in static/network analysis, Malware.

He co-founded and organizes @sec_wakate, a community for junior security engineers in Japan. He has spoken at Black Hat USA/Asia Arsenal, AVTOKYO, and AWS Security JAWS.

SpeakerBio: hikae

Security Engineer in Red Team @ freee inc, AI Security Specialist.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: sisakulint:CI-Friendly static linter with autofix, SAST, semantic analysis for GitHub Actions

Tags: AI | DEF CON Demo Labs | Intermediate | AppSec | Cloud | DevOps | Purple Team | DEF CON Demo Labs

When: Saturday, Aug 8, 11:00 - 11:45 PDT

Where: LVCCW Level 1 Hall 3 1002 (Demo Labs Track 2) - [Map](#)

Description:

GitHub Actions workflows are vulnerable by default. Hardening such as commit-hash pinning, least-privilege permissions, and timeouts is optional, never enforced at pipeline level. Exploitable configs ship daily, increasingly written by Coding Agents. sisakulint is a fast heuristic static analyzer for GitHub Actions covering all OWASP Top 10 CI/CD risks, with 52 rules, a taint engine, and 38+ auto-fixes. It outpaces CodeQL on speed and quality, with 100% detection on 18 GHSL advisories and 81.6% on 38 GHSA covering exploits in PX4-Autopilot, vets-api, weaviate, nrwl/nx.

Impostor Commit at CVSS 9.8 validates pinned SHAs against the claimed repository, not impostors via Git forks, a check unique to sisakulint. Code Injection at CVSS 9.8 tracks untrusted input through ``${}`` and step outputs. AI Action Rules detect Clinejection on claude-code-action, copilot-swe-agent, and openai-actions, covering tool grants, prompt injection, and wildcard triggers, as in Cline 2026/02 where issue title injection stole NPM_RELEASE_TOKEN. Known Vulnerable Actions catches tj-actions/changed-files.

In the Coding Agent era, linters matter more. Delegating 52 rules to an LLM degrades precision; deterministic engines run in ms with no variance. The session covers end-to-end detection, taint propagation, and automated remediation.

Speakers: Atsushi Sada, hikae

SpeakerBio: Atsushi Sada

Atsushi Sada is a CSIRT member specializing in cloud security on AWS and GitHub, and enterprise security with MDM, EDR, AI governance. He is an ethical hacker and security tool developer. He built sisakulint and MachStealer for practical security research in static/network analysis, Malware.

He co-founded and organizes @sec_wakate, a community for junior security engineers in Japan. He has spoken at Black Hat USA/Asia Arsenal, AVTOKYO, and AWS Security JAWS.

SpeakerBio: hikae

Security Engineer in Red Team @ freee inc, AI Security Specialist.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Six Impossible Things Before Breakfast: Common Misconceptions About Being a CTI Analyst

Tags: Noob Community | Creator Talk/Panel

When: Saturday, Aug 8, 15:00 - 15:59 PDT

Where: LVCCW Level 1 Hall 4 1417 (Noob Community) - [Map](#)

Description:

"Why, sometimes I've believed as many as six impossible things before breakfast." So said the White Queen to Alice — and so says the cybersecurity community about what it means to work in cyber threat intelligence.

The cyber threat intelligence (CTI) domain is rich with acronyms, niche frameworks, specialized tools, and diverse practitioners — and for newcomers, whether they are making a career change or just starting, that richness can feel more like a labyrinth than an invitation. From engaging with novice analysts at industry conferences and through diversity and inclusion programs like Cyversity, to teaching at the undergraduate level, I've found that a consistent set of misconceptions keeps talented, curious people from ever walking through the door. And that's a problem, because CTI needs those people.

This presentation will guide attendees down the rabbit hole and into the CTI domain, starting with a primer on intelligence history and the intelligence lifecycle before tackling six of the most persistent myths head-on: that you need deep technical expertise to succeed; that CTI only exists in government; that the job is just monitoring feeds and social media; that you'll spend your career writing endless reports; that success requires mastering thousands of tools; and that automation will eventually make analysts obsolete. Each misconception will be examined, dismantled, and replaced with a clearer picture of what the work actually looks like — and why diverse, non-traditional backgrounds don't just belong in CTI, they make it stronger.

Attendees will leave with a grounded understanding of the CTI domain, a realistic sense of what the role demands, and concrete first steps for getting involved — whether they're a seasoned professional exploring a pivot or a complete newcomer who just learned what "CTI" stands for five minutes ago.

(outline below)

Title Slide [< 1 min] Presentation Disclaimers [< 1 min] Agenda [< 1 min] Speaker Introduction [2 min]

Down the Rabbit Hole: Cyber Threat Intelligence Primer [4 mins] Foundations of the cyber threat intelligence domain
Intelligence history and lifecycle

The White Rabbit: You Will Not Succeed without a Technical Background [6 mins] Non-technical skills, such as written and verbal communication, are equally important. Problem-solving and pattern recognition are key to collaborating with other technical teams. Still, you do not need the same skills as members of those teams, i.e. detection engineering or malware reverse engineering. Continuous learning for upskilling

We're All Mad Here: CTI is Only Used in the Government [6 mins] Most private enterprises also embed cyber threat intelligence teams' practices within their cybersecurity operations department. Use cases: fraud and payments intelligence in financial services; tracking threat actors' abuse of consumer-facing services and platforms in the technology sector; monitoring disruptive threat activity in critical infrastructure businesses Cross-industry sharing and collaboration

Tweedledee and Tweedledum: You're Just Monitoring Threat Feeds and Social Media [6-8 mins] CTI is a multi-faceted field and involves more than "eyes-on-glass" monitoring. Examples of other areas of focus: Campaign analysis Operational research and correlation of threat actor behaviors with other cybersecurity teams Threat infrastructure hunting and pivoting Threat communication and influencing

The Mad Hatter's Tea Party: Endless Report Writing [6 mins] Stakeholder communication preferences usually dictate threat intelligence output Some stakeholders may prefer visual communications (presentations, one-pagers, system dashboards) over written reports. Other stakeholders may prefer brief tactical updates via Teams/Slack or notes added to a SOAR platform.

The Queen of Hearts' Rules: Your Success Hinges on Knowing Thousands of Tools [6 mins] Tools will come and go, but methodology and critical thinking are more important Prioritize understanding how to perform analysis, leverage intelligence frameworks, influence stakeholders, and collaborate with others over learning an individual tool.

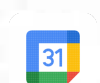
Humpty Dumpty was Confidently Wrong: CTI Can be Fully Automated [8 mins] Automation plays a pivotal role but cannot outright replace analysts who support the domain. Scripts can help eliminate mundane tasks. Applying CTI adequately anchors on qualitative assessments and knowledge of an enterprise's security posture Applications of AI in CTI AI could help welcome more diverse CTI practitioners by breaking down barriers to entry due to the required technical skill set.

Summary [5 mins] Getting started today

Q&A [Remaining Time]

SpeakerBio: Brett Tolbert

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Bug Bounty Village - Sunday - 10:00-10:30 PDT

Title: Skill Issue: A Recon Story

Tags: Bug Bounty Village | Creator Talk/Panel

When: Sunday, Aug 9, 10:00 - 10:30 PDT

Where: LVCCW Level 1 Hall 3 1102 (Creator Stage 6) - [Map](#)

Description:

For ten years we told every hunter the same thing: learn the bug classes, grind the labs, memorize the payloads. It built a generation of hackers, and the perfect training set. Every writeup, every PayloadsAllTheThings entry, every CTF solution is now fuel for a model. We documented exploitation so well that we automated ourselves out of the easy half of the job.

I'm not mad about it. It was always going to happen. The bottom of the funnel, the known classes on known surfaces, belongs to the swarm now. If your edge is running the same templates against the same assets, you are racing a machine that never sleeps. You lose that race.

So where did the human edge go? Upstream. To recon.

Recon never got written down the way exploitation did. The intro stuff did: run these five tools, pipe it into httpx. But the part that actually finds the bug, the judgment about which of forty thousand assets is worth your night, the instinct for where an org cut a corner, the pivots that surface the forgotten staging box, that part lives in people's heads. It is tribal. It moves through private channels and bar talk at cons. A model cannot train on what was never published.

Recon is the last moat, and the moat is built from information asymmetry, not skill. It keeps paying not because hunters are smarter than the bots, but because hunters know things the bots were never told. Every time someone publishes a technique, the moat drains a little. It refills faster than it drains, because the people who hold the best recon rarely have a reason to write it down.

I will make that concrete, not philosophical: the categories of recon that resist documentation, why scanners miss them (tools enumerate, humans interpret), and where to point your attention in 2026. Then I give away one or two techniques not in the standard rotation, walked end to end, with the reasoning, not just the command. You leave with something you can use that night.

SpeakerBio: Ryan Bonner, Lead Security Engineer at Arcanum Information Security

Ryan Bonner is a Lead Security Engineer at Arcanum Information Security, where he builds AI systems, hacks them, and runs application penetration tests. Off the clock he hunts wide-scope bug bounty programs.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Noob Community - Saturday - 10:00-17:59 PDT

Title: Skillbit Labs

Tags: Noob Community | Creator Event/Activity

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 4 1417 (Noob Community) - [Map](#)

Description:

SkillBit Labs is a continuous learning platform designed to help assess and develop cybersecurity skills through hands-on, bite-sized labs. Drop in during village hours and work through beginner-friendly challenges at your own pace, brought to you by SkillBit (formerly MetaCTF), led by CEO Roman Bohuk.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Noob Community - Friday - 10:00-17:59 PDT

Title: Skillbit Labs

Tags: Noob Community | Creator Event/Activity

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 4 1417 (Noob Community) - [Map](#)

Description:

SkillBit Labs is a continuous learning platform designed to help assess and develop cybersecurity skills through hands-on, bite-sized labs. Drop in during village hours and work through beginner-friendly challenges at your own pace, brought to you by SkillBit (formerly MetaCTF), led by CEO Roman Bohuk.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Noob Community - Sunday - 10:00-13:59 PDT

Title: Skillbit Labs

Tags: Noob Community | Creator Event/Activity

When: Sunday, Aug 9, 10:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 4 1417 (Noob Community) - [Map](#)

Description:

SkillBit Labs is a continuous learning platform designed to help assess and develop cybersecurity skills through hands-on, bite-sized labs. Drop in during village hours and work through beginner-friendly challenges at your own pace, brought to you by SkillBit (formerly MetaCTF), led by CEO Roman Bohuk.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Payment Village - Friday - 12:00-12:45 PDT

Title: Skimmers, Shimmers, and You

Tags: Payment Village | Creator Talk/Panel

When: Friday, Aug 7, 12:00 - 12:45 PDT

Where: LVCCW Level 2 W204-205 (Payment Village) - [Map](#)

Description:

Join me as I present my latest research on fraudulent payment devices such as card skimmers and shimmers, building on insights from close collaboration with major retailers, law enforcement, and the United States Secret Service! I will outline the evolving landscape of payment threats and share findings from my hands-on reverse engineering of over 130 fraudulent devices, including ATM, fuel pump, and both point-of-sale skimmers and shimmers. Learn why reliably detecting skimmers is challenging and the latest tools and techniques used to both spot and conceal these malicious devices. Peek behind the curtain of payment security with me to explore how cards are cloned and contactless payments relayed from across the world. You'll learn how skimmers disproportionately affect U.S. citizens on government benefits and ways to best protect yourself in the ever-changing landscape of digital payments!

SpeakerBio: Aidan Quimby, Senior Consultant, Coalfire DivisionHex

Specializes in web app pentesting, payment-skimmer forensics and hardware hacking; previously led hardware testing at IBM X-Force Red and has presented skimmer research to major retailers and at Hardwear.io.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Sliding into the Flight Deck's DMs: Practical Message Attacks on CPDLC

Tags: DEF CON Official Talk | Exploit

When: Friday, Aug 7, 11:00 - 11:59 PDT

Where: LVCCW Level 1 Hall 3 903 (Main Track 5) - [Map](#)

Description:

Air traffic control quietly moved from voice radios to text messages—and almost nobody outside aviation noticed.

We did. And it turns out you can slide into a commercial aircraft's DMs.

In this talk, we show how modern aircraft receive digital instructions (like “climb,” “descend,” or “turn”) over a system called CPDLC—and how that system has basically zero real security. No crypto. No authentication. Just vibes and protocol complexity.

We built a full fake ground station using cheap SDR gear and made certified avionics believe we were air traffic control. From there, we can inject real flight instructions or knock aircraft offline at scale with protocol-level DoS attacks—no jamming required.

This isn't a simulation. We tested it against real aviation hardware in a live CPDLC environment.

If you've ever wondered what happens when safety-critical infrastructure assumes “nobody will try this,” this talk is for you.

Sliding into the Flight Deck's DMs: Practical Message Attacks on CPDLC

Mehdi Ziazi, ETH Zurich; Khalid Aleem, Independent; Harshad Sathaye, ETH Zurich; Martin Strohmeier, Cyber-Defence Campus, armasuisse Science + Technology

Usenix Security 2026

Speakers: Martin "MasorX" Strohmeier, Mehdi Ziazi

SpeakerBio: Martin "MasorX" Strohmeier, Cyber-Defence Campus, armasuisse Science + Technology

Martin is a Senior Scientist at the Swiss Cyber Defence Campus, primarily based at ETH Zurich, and a Visiting Fellow of Kellogg College, Oxford. His work focuses on designing and analyzing security protocols for cyber-physical systems in critical infrastructures—aviation, satellites, space, and transportation systems. Martin also explore privacy issues in global networks, adversarial machine learning, and open-source intelligence.

Martin received his DPhil in 2016 at Oxford, supervised by Prof. Ivan Martinovic, where he studied the security and privacy of aviation communication technologies. I co-founded the OpenSky Network and coordinate its research activities. His work has received awards from both the aviation and security communities, including the EPSRC Doctoral Prize Fellowship and commendation from the British Computer Society. Martin has published regularly at all major security and AI conferences and also been a speaker at DEF CON several times (main stage + villages).

SpeakerBio: Mehdi Ziazi, ETH Zurich

Mehdi Ziazi is a hacker and cybersecurity student at ETH Zurich and an incoming PhD student at CISPA focused on aerospace security and cyber-physical systems. Their recent work in aviation security explores novel attack paths against aircraft systems and their real-world impact, approached with curiosity, persistence, and a bit of stubbornness.



Bug Bounty Village - Sunday - 10:30-10:59 PDT

Title: Slop Spotting, Using Rules to Detect AI Slop for Bug Bounty

Tags: Bug Bounty Village | Creator Talk/Panel

When: Sunday, Aug 9, 10:30 - 10:59 PDT

Where: LVCCW Level 1 Hall 3 1102 (Creator Stage 6) - [Map](#)

Description:

curl ended its HackerOne programme in January 2026 after a steep rise in AI-generated reports overwhelmed a seven-person security team, with some weeks seeing seven reports in sixteen hours, none valid. They were all AI generated; referencing lines of code, real vulnerabilities, and regression of resolved CVEs, they looked legitimate and if that code was actually in the project would have been valid. Every single report wasted the maintainers time and the platform they were using did nothing to help. Triaging them is expensive, slow, and demoralising for the humans at the other end, the only solution? Pay the platform to triage them for you. This talk introduces Slop Spotting: a lightweight triage methodology that uses SAST rule generation as a validity signal. The core insight is simple. If a vulnerability is real and well-specified, you should be able to write a SAST rule for it, and if that code is actually in the codebase, that SAST rule should have a result, if it's slop, even convincing slop you get a yes/no answer very quickly across even large codebases.

Speakers:Katie Paxton-Fear,Max vonBlankenburg

SpeakerBio: Katie Paxton-Fear, Security Advocate, Semgrep

i used to make applications and now I break them, hacker, bug bounty hunter, and educational YouTuber.

SpeakerBio: Max vonBlankenburg, Security Researcher, Semgrep

Max is a security research engineer at Semgrep, doing their best to make software break less. Max has worked with smart contracts, CTFs and the software supply chain. Right now they're interested in how to use AI to help make security engineering easier and tip the scales towards defenders.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Slopcon

Tags: Event

When: Friday, Aug 7, 22:00 - 00:59 PDT

Where: LVCCW Level 2 W222 (Workshops) - [Map](#)

Description:

In an era where "innovation" is just a polite word for scraping the bottom of the LLM barrel, we invite you to embrace the inevitable heat death of original thought at Slopcon. Why bother with pesky human intellect when we can automate the entire conference lifecycle, from hallucinated CFP submissions to slide decks that make absolutely no sense? It's a high-stakes experiment in synthetic absurdity where the only thing more artificial than the intelligence is the confidence of the "meatbag" presenters tasked with delivering this digital dross. Join us for a celebratory descent into the uncanny valley, where we'll crown the sloppiest generative disasters and toast to the fact that, for now, at least the audience is still real.

So, if you're actually itching to subject the world to more of this or just have a masochistic need for further details, head over to slopcon.org and fulfill your destiny.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Smart Contracts, Smarter Malware: Automating Recon on Blockchain-Based C2

Tags: Malware Village | Creator Talk/Panel

When: Friday, Aug 7, 14:05 - 14:45 PDT

Where: LVCCW Level 1 Hall 2 600 (Malware Village) Talks - [Map](#)

Description:

Threat actors are moving their command-and-control (C2) infrastructure to the blockchain, where smart contracts are immutable, globally accessible, and completely immune to traditional takedowns. Instead of reaching out to attacker-controlled servers, modern malware families query public blockchain RPC endpoints to retrieve C2 instructions written directly into smart contracts across a variety of ecosystems. No attacker server, no domain to seize, no hosting provider to contact.

In this talk, we break down our investigation into malware families actively utilizing multi-chain smart contracts as an evasive C2 channel. We will cover how we analyzed network traffic to identify decentralized communication patterns, queried live contract methods to extract real-time C2 data, and used cross-chain bytecode analysis to map shared infrastructure across multiple samples.

We will demonstrate a unified framework that consolidates these individual recon methodologies, automating the extraction, tracking, and reverse-engineering of multi-chain blockchain-based malware infrastructure.

Speakers: Sai Sathvik Rupp, Chris Navarrete

SpeakerBio: Sai Sathvik Rupp, Staff Security Researcher at Palo Alto Networks

Sai Sathvik Rupp is a Staff Security Researcher at Palo Alto Networks and a recent M.S. graduate in Information Security from Carnegie Mellon University. He specializes in vulnerability detection and malware analysis, leveraging his expertise to identify, analyze, and mitigate advanced cyber threats.

SpeakerBio: Chris Navarrete, Senior Principal Security Researcher - CDSS Advanced Threat Prevention (ATP) at Palo Alto Networks

Chris Navarrete is a Senior Principal Security Researcher within the Advanced Threat Prevention team at Palo Alto Networks. His work centers on cutting-edge research in cybersecurity, particularly in threat detection and malware analysis. Previously, he served as an adjunct professor of computer science at San Jose State University, teaching Software Security Technologies. He holds a Master of Science in software engineering with a specialization in cybersecurity from San Jose State University. Chris has presented at major industry conferences, including Black Hat Asia, the Computer Antivirus Research Organization (CARO), the Cyber Threat Alliance's Threat Intelligence Practitioners (TIPS) conference, and Black Hat Arsenal, where he introduced and released BLACKPHENIX — a framework designed to automate malware analysis workflows.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

IoT Village - Sunday - 10:00-13:59 PDT

Title: Smart Home in the Matter: Blink, Race, Attack CTF

Tags: IoT Village | Creator Event/Activity

When: Sunday, Aug 9, 10:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 1 215 (IoT Village) - [Map](#)

Description:

Bitdefender and Netgear invite you into the smart-home arena, where the Matter fabric pulses with secrets, traps, and unexpected twists, and where AI can finally take a break while your critical thinking takes the lead.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

IoT Village - Friday - 10:00-17:59 PDT

Title: Smart Home in the Matter: Blink, Race, Attack CTF

Tags: IoT Village | Creator Event/Activity

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 215 (IoT Village) - [Map](#)

Description:

Bitdefender and Netgear invite you into the smart-home arena, where the Matter fabric pulses with secrets, traps, and unexpected twists, and where AI can finally take a break while your critical thinking takes the lead.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

IoT Village - Saturday - 10:00-17:59 PDT

Title: Smart Home in the Matter: Blink, Race, Attack CTF

Tags: IoT Village | Creator Event/Activity

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 215 (IoT Village) - [Map](#)

Description:

Bitdefender and Netgear invite you into the smart-home arena, where the Matter fabric pulses with secrets, traps, and unexpected twists, and where AI can finally take a break while your critical thinking takes the lead.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Smile, you're on camera! Livestreaming from North Korea's IT workers laptop farm

Tags: DEF CON Official Talk | Demo

When: Saturday, Aug 8, 15:00 - 15:59 PDT

Where: LVCCW Level 1 Hall 3 903 (Main Track 5) - [Map](#)

Description:

We infiltrated a cell of North Korean IT workers dedicated to obtaining remote employment for the DPRK, attributed to Famous Chollima (Lazarus Group). Posing as facilitators, we went through their full recruitment process and, once inside, provided them with controlled environments that allowed us to observe and record their operations from the inside.

In parallel, we used OSINT and targeted reconnaissance to map their infrastructure, track financial movements, and reconstruct the broader structure behind the operation. This includes networks of fake companies and identities, local facilitators, fraudulent H-1B visa schemes, and a coordinated model of transnational fraud used to gain access to Western companies.

The talk features recorded direct interactions with DPRK operatives and live recordings from a fake laptop farm we built for them. While they believed they had remote access to legitimate work systems, we captured everything: how they set up their infrastructure, handled authentication, configured VPNs, and operated on a daily basis.

This was the first time this kind of threat campaign was profiled, recorded, and published from the inside. Now we want to share it with you. Smile, you're on camera!

Original article: - <https://any.run/cybersecurity-blog/lazarus-group-it-workers-investigation/>

Media: -
<https://www.bleepingcomputer.com/news/security/north-korea-lures-engineers-to-rent-identities-in-fake-it-worker-scheme/> -
<https://thehackernews.com/2025/12/researchers-capture-lazarus-apt-remote.html>

Speakers: Heiner García, Mauro Eldritch

SpeakerBio: Heiner García, NorthScan

Researcher & Strategic intelligence Analyst

Founder of NorthScan

Cyber Threat Intelligence at Telefonica Tech

SpeakerBio: Mauro Eldritch, Leader at Bitso Quetzal Team

Hacker and Speaker.

Founder of BCA LTD and DC5411.

I wrote a book interviewing Threat Actors.

I like Threat Intelligence and Golden Retrievers.



Biohacking Village - Friday - 15:45-16:30 PDT

Title: Snap, Crackle, Popped: How to manage a massive cyber attack

Tags: Biohacking Village | Creator Talk/Panel

When: Friday, Aug 7, 15:45 - 16:30 PDT

Where: LVCCW Level 1 Hall 3 1105 (Creator Stage 3) - [Map](#)

Description:

First hand account of the inner workings of a massive breach, what works what does not and where the wheels fall off the bus quick.

SpeakerBio: David Nathans

David Nathans is a senior cybersecurity executive and former U.S. Air Force cyber officer. He has served as a Global CISO in highly regulated industries and is an entrepreneur, author, and advisor focused on security operations, Zero Trust, and risk governance.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Ham Radio Village - Saturday - 12:00-12:30 PDT

Title: So You Got Your License, Now What?

Tags: Ham Radio Village | Creator Talk/Panel

When: Saturday, Aug 8, 12:00 - 12:30 PDT

Where: LVCCW Level 3 W315 (Ham Radio Village) - [Map](#)

Description:

Getting your ham radio license is the easy part. Figuring out what to do next? That's where most people get stuck. This talk is a practical, opinionated guide to the best rabbit holes in amateur radio: satellites, APRS, HF operating, digital modes, antenna experimentation, POTA, and the beautiful chaos of Field Day. Whether you got your ticket last week or you've been meaning to upgrade for years, this is an opinionated romp through the hobby.

We'll cover the stuff no one tells you after the exam: what the bands actually feel like, why FT8 will make you productive and vaguely empty inside, how much you can accomplish with \$50 of wire and a willingness to climb things, and why learning to solder is basically a superpower. We'll also talk about getting off the couch comms for events and contests like POTA and ARRL Field Day are the most chaotic fun you can have with a radio legally.

It's easy to listen, but things get more interesting when you start transmitting. Ham radio is one of the last hobbies that rewards you for actually understanding how it works. This talk is the map.

You crammed, you passed, you got a callsign. And now your radio is sitting in a box while you wonder what you're actually supposed to do with it. This talk is a guided tour of the rabbit holes waiting for you on the other side of your license exam, organized by how deep you want to fall. Technician class? You can hit satellites with a handheld, track yourself on a map with APRS, or chase hidden transmitters through the woods with a directional antenna and questionable judgment. Upgrade to General and suddenly you've got the HF bands: a global playground where you can work 200 countries in a weekend via a mode a Nobel laureate invented, argue with the laws of physics via antenna wire, and wage legal warfare against your HOA.

SpeakerBio: Danny Quist

Danny Quist has been a licensed amateur radio operator since he was 17, which is a really long time. Currently he is an extra class operator who gets to operate in his freetime working as CTO at Swarm Inc. He is a volunteer examiner with the ham radio village. His day job includes reverse engineering malware, forward engineering malware detonation systems, and management.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: So You Want to Be a Red Teamer? The Reality Behind the Role

Tags: Noob Community | Creator Talk/Panel

When: Sunday, Aug 9, 11:45 - 12:15 PDT

Where: LVCCW Level 1 Hall 4 1417 (Noob Community) - [Map](#)

Description:

If you spend enough time online, you might think red teaming is all zero-days, custom malware, and elite operators silently dismantling networks while dramatic music plays in the background.

The reality is very different.

Modern red team operations are less about “cool hacks” and more about planning, communication, and helping organizations improve their defenses. In many cases, the most important skills have nothing to do with hacking at all.

This talk is designed for newcomers interested in offensive security who want an honest look at what red teamers actually do, how engagements are planned, what skills matter most, and how to begin building a realistic path into the field.

We'll break down the differences between penetration testing and red/purple teaming, discuss common misconceptions about offensive security careers, and explore a real-world red team engagement from planning through debrief.

If you've ever wondered what red teamers really do, this session is for you.

SpeakerBio: Billy Giles

Billy Giles is an Offensive Security leader and practitioner who specializes in red/purple teaming and network penetration testing. With a deep passion for understanding adversary behaviors, he helps organizations across a multitude of industries assess their security postures, identify and remediate vulnerabilities, and build stronger defenses by thinking like an attacker.

Billy is also the creator of Thinking Offensively. Through this project he examines offensive security strategy topics to help cybersecurity leaders anticipate threats and inform decision making, while also providing tools, playbooks, and techniques that red teams can apply directly to their work. His mission is to bridge strategy and execution to help organizations think offensively and stay ahead of evolving threats.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Aerospace Village - Saturday - 11:30-11:59 PDT

Title: So You Want to Work in Aircraft Cyber? Here's what you need to know!

Tags: Aerospace Village | Creator Talk/Panel

When: Saturday, Aug 8, 11:30 - 11:59 PDT

Where: LVCCW Level 1 Hall 3 1103 (Creator Stage 5) - [Map](#)

Description:

As the Aviation industry struggles to recruit people with the right combination of knowledge and/or experience of Cybersecurity and Aviation ecosystems, this presentation will provide a very fast overview of the topics people wishing to break into the industry should consider learning more about. This will be a fast-fire and frank presentation with direction for you to start your journey into Aviation Cyber.

Speakers: Matt Gaffney, Marcie Wise

SpeakerBio: Matt Gaffney

No BIO available

SpeakerBio: Marcie Wise

No BIO available

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Telecom Village - Friday - 11:00-12:30 PDT

Title: SOC Threat Hunting in Practice

Tags: Telecom Village | Creator Talk/Panel

When: Friday, Aug 7, 11:00 - 12:30 PDT

Where: LVCCW Level 3 W321 (Telecom Village) - [Map](#)

Description:

Theory 1. Integrating modern SOC with Telco and respective component

Theory 2. Key Attack identifier

Demo 1: Ran Site attack identification in Morden SOC Tool

Demo 2: 5g Core threat identification for insider attack

Practical : Hunting for attack pattern, identify attacker traces, impact analysis on overall network infra

SpeakerBio: Akib Sayyed

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Social Engineering 101: The Four Psychological Backdoors to Scam Your Way into Anything

Tags: Social Engineering Community Village | Creator Event/Activity

When: Saturday, Aug 8, 10:00 - 10:59 PDT

Where: LVCCW Level 3 W320 (Social Engineering Community Village Labs) - [Map](#)

Description:

Social engineering not just a specialized skill used by elite hackers, professional con artists, or unnervingly charismatic strangers. In reality, the same few psychological vulnerabilities show up everywhere: in negotiations, job interviews, sales pitches, security breaches, party tricks, and everyday conversations...

And YOU can use them, too.

In this interactive session, magician and social-engineering educator Brian Brushwood reveals four psychological backdoors that can make people more likely to trust, comply, disclose, and cooperate. You will see each principle demonstrated, learn why it works, and practice using it through safe, low-stakes exercises with other attendees.

These are the tricks that can be used by good guys and bad to convince, and build rapport quickly, lower resistance, and make an unlikely request feel surprisingly reasonable.

By learning how these techniques feel from the inside, attendees will become better at using influence deliberately, and better at recognizing when someone is using it on them.

No previous social-engineering experience is required. Just bring a willingness to talk to strangers, learn a magic trick or two, and discover how alarmingly hackable human beings really are.

SpeakerBio: Brian Brushwood

Brian Brushwood has spent 25 years teaching millions of people how deception works: first as a touring magician, then as creator/host of Scam School / Scam Nation, host of National Geographic's Hacking the System, creator of The Modern Rogue, and host of World's Greatest Con. His work focuses on scams, magic, persuasion, social engineering, and the mechanics of trust: how it is built, exploited, defended, and rehearsed. Through Scam School and Scam Nation, Brian spent nearly two decades turning ordinary non-deceivers into capable ethical deceivers, helping them understand cons and persuasion from the inside. Brian has delivered keynotes to audiences of thousands and recently developed an experimental offense-to-defense social engineering curriculum, piloted at Clemson University with CISO John Hoyt.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Social Engineering 101: The Four Psychological Backdoors to Scam Your Way into Anything

Tags: Social Engineering Community Village | Creator Event/Activity

When: Saturday, Aug 8, 11:30 - 12:30 PDT

Where: LVCCW Level 3 W320 (Social Engineering Community Village Labs) - [Map](#)

Description:

Social engineering not just a specialized skill used by elite hackers, professional con artists, or unnervingly charismatic strangers. In reality, the same few psychological vulnerabilities show up everywhere: in negotiations, job interviews, sales pitches, security breaches, party tricks, and everyday conversations...

And YOU can use them, too.

In this interactive session, magician and social-engineering educator Brian Brushwood reveals four psychological backdoors that can make people more likely to trust, comply, disclose, and cooperate. You will see each principle demonstrated, learn why it works, and practice using it through safe, low-stakes exercises with other attendees.

These are the tricks that can be used by good guys and bad to convince, and build rapport quickly, lower resistance, and make an unlikely request feel surprisingly reasonable.

By learning how these techniques feel from the inside, attendees will become better at using influence deliberately, and better at recognizing when someone is using it on them.

No previous social-engineering experience is required. Just bring a willingness to talk to strangers, learn a magic trick or two, and discover how alarmingly hackable human beings really are.

SpeakerBio: Brian Brushwood

Brian Brushwood has spent 25 years teaching millions of people how deception works: first as a touring magician, then as creator/host of Scam School / Scam Nation, host of National Geographic's Hacking the System, creator of The Modern Rogue, and host of World's Greatest Con. His work focuses on scams, magic, persuasion, social engineering, and the mechanics of trust: how it is built, exploited, defended, and rehearsed. Through Scam School and Scam Nation, Brian spent nearly two decades turning ordinary non-deceivers into capable ethical deceivers, helping them understand cons and persuasion from the inside. Brian has delivered keynotes to audiences of thousands and recently developed an experimental offense-to-defense social engineering curriculum, piloted at Clemson University with CISO John Hoyt.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Social Engineering Community Village - Open Hours

Tags: Social Engineering Community Village | Creator Event/Activity

When: Sunday, Aug 9, 10:00 - 12:30 PDT

Where: LVCCW Level 3 W317-319 (Social Engineering Community Village) - [Map](#)

Description:

Morning, social engineers! Swing by for your SEC merch, claim your seat, and prepare for action... the phones start ringing soon.

The Social Engineering Community village dives into one of the most powerful attack surfaces in security: humans. Our village creates a space where attendees can explore the psychology, tactics, and tradecraft behind human-focused hacking. Through presentations, live demonstrations (via contests), and interactive activities, students, defenders, hackers, and the curious can see how reconnaissance, persuasion, and improvisation are used to bypass even the best defenses.

At DEF CON the village becomes a live stage for the craft. In the Social Engineering Community Vishing Competition (SECVV), competitors step into a soundproof booth and place real calls using OSINT, creative pretexts, and quick thinking while the audience watches the strategy unfold in real time. In Battle of the Bots, human-created AI agents attempt social engineering calls of their own, exploring what happens when automated systems try their hand at elicitation. Alongside the contests, attendees can have the opportunity to place calls in our "Cold Calls" or listen in to some presentations.

The village is built by the community that practices the craft. Volunteers, researchers, hackers, defenders, and curious newcomers all contribute to the content each year, creating space for new voices and ideas to take the stage. Whether you want to watch live un-scripted social engineering calls, understand the psychology behind it, or meet others who love the human side of security, the Social Engineering Community village is the place to experience it at DEF CON.

Prerequisites:

Attendees are welcome to watch contests, join discussions, and participate in interactive activities with no preparation needed.

Competitors in the Social Engineering Community Vishing Competition and Battle of the Bots Contest are selected in advance through a Call for Competitors prior to DEF CON, but some activities such as Cold Calls allow audience members to sign up onsite and participate.

Attendees who want to participate in Cold Calls may benefit from brushing up on basic social engineering skills such as rapport building, influence and elicitation techniques.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Social Engineering Community Village - Open Hours

Tags: Social Engineering Community Village | Creator Event/Activity

When: Friday, Aug 7, 08:30 - 17:59 PDT

Where: LVCCW Level 3 W317-319 (Social Engineering Community Village) - [Map](#)

Description:

Morning, social engineers! Swing by for your SEC merch, claim your seat, and prepare for action... the phones start ringing soon.

The Social Engineering Community village dives into one of the most powerful attack surfaces in security: humans. Our village creates a space where attendees can explore the psychology, tactics, and tradecraft behind human-focused hacking. Through presentations, live demonstrations (via contests), and interactive activities, students, defenders, hackers, and the curious can see how reconnaissance, persuasion, and improvisation are used to bypass even the best defenses.

At DEF CON the village becomes a live stage for the craft. In the Social Engineering Community Vishing Competition (SECVV), competitors step into a soundproof booth and place real calls using OSINT, creative pretexts, and quick thinking while the audience watches the strategy unfold in real time. In Battle of the Bots, human-created AI agents attempt social engineering calls of their own, exploring what happens when automated systems try their hand at elicitation. Alongside the contests, attendees can have the opportunity to place calls in our "Cold Calls" or listen in to some presentations.

The village is built by the community that practices the craft. Volunteers, researchers, hackers, defenders, and curious newcomers all contribute to the content each year, creating space for new voices and ideas to take the stage. Whether you want to watch live un-scripted social engineering calls, understand the psychology behind it, or meet others who love the human side of security, the Social Engineering Community village is the place to experience it at DEF CON.

Prerequisites:

Attendees are welcome to watch contests, join discussions, and participate in interactive activities with no preparation needed.

Competitors in the Social Engineering Community Vishing Competition and Battle of the Bots Contest are selected in advance through a Call for Competitors prior to DEF CON, but some activities such as Cold Calls allow audience members to sign up onsite and participate.

Attendees who want to participate in Cold Calls may benefit from brushing up on basic social engineering skills such as rapport building, influence and elicitation techniques.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Social Engineering Community Village - Open Hours

Tags: Social Engineering Community Village | Creator Event/Activity

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 3 W317-319 (Social Engineering Community Village) - [Map](#)

Description:

Morning, social engineers! Swing by for your SEC merch, claim your seat, and prepare for action... the phones start ringing soon.

The Social Engineering Community village dives into one of the most powerful attack surfaces in security: humans. Our village creates a space where attendees can explore the psychology, tactics, and tradecraft behind human-focused hacking. Through presentations, live demonstrations (via contests), and interactive activities, students, defenders, hackers, and the curious can see how reconnaissance, persuasion, and improvisation are used to bypass even the best defenses.

At DEF CON the village becomes a live stage for the craft. In the Social Engineering Community Vishing Competition (SECVV), competitors step into a soundproof booth and place real calls using OSINT, creative pretexts, and quick thinking while the audience watches the strategy unfold in real time. In Battle of the Bots, human-created AI agents attempt social engineering calls of their own, exploring what happens when automated systems try their hand at elicitation. Alongside the contests, attendees can have the opportunity to place calls in our "Cold Calls" or listen in to some presentations.

The village is built by the community that practices the craft. Volunteers, researchers, hackers, defenders, and curious newcomers all contribute to the content each year, creating space for new voices and ideas to take the stage. Whether you want to watch live un-scripted social engineering calls, understand the psychology behind it, or meet others who love the human side of security, the Social Engineering Community village is the place to experience it at DEF CON.

Prerequisites:

Attendees are welcome to watch contests, join discussions, and participate in interactive activities with no preparation needed.

Competitors in the Social Engineering Community Vishing Competition and Battle of the Bots Contest are selected in advance through a Call for Competitors prior to DEF CON, but some activities such as Cold Calls allow audience members to sign up onsite and participate.

Attendees who want to participate in Cold Calls may benefit from brushing up on basic social engineering skills such as rapport building, influence and elicitation techniques.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Social Gatherings/Events - Friday - 19:00-22:59 PDT

Title: Social Engineering Community Village Party

Tags: Party | Social Engineering Community Village

When: Friday, Aug 7, 19:00 - 22:59 PDT

Where: LVCCW Level 3 W317-319 (Social Engineering Community Village) - [Map](#)

Description:

Mix and mingle with the SEC crew, competitors, speakers, and fellow attendees at our community party.

Join the Social Engineering Community for a night of connecting with fellow hackers, social engineers, researchers, and curious DEF CON attendees who share an interest in the human side of hacking. Whether you spent the weekend watching vishing calls, cheering on AI bots, competing, volunteering, or just discovering the craft for the first time, this meetup is a chance to relax, swap stories, and meet the people behind the voices, research, and chaos from the village. The exact theme will be announced soon, but the goal is simple: bring the community together, make new friends, reconnect with old ones, and celebrate another year of social engineering at DEF CON. Everyone is welcome, whether you're a longtime member of the community or just curious about what social engineering is all about.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Red Team Village - Friday - 14:00-15:59 PDT

Title: Social Engineering With Reel

Tags: Red Team Village | Misc

When: Friday, Aug 7, 14:00 - 15:59 PDT

Where: LVCCW Level 1 Hall 1 309 (Red Team Village) Tactic Table 4 - [Map](#)

Description:

Reel is a modern social engineering framework, developed for use by the TrustedSec Targeted Ops team. It supports phishing campaigns, proxying captured credentials to other sites, device code phishing, dynamic SMS and voice campaigns (via integration with AWS). This session will show the attendees how deploy and configure reel, as well as how to craft advanced SE campaigns using the reel workflow system and show how custom plugins can be developed.

SpeakerBio: James Williams

James is a senior consultant on the Targeted Operations team at TrustedSec. He has around 10 years experience in cyber security, including penetration testing and red team roles. In his spare time, James enjoys running over mountains (it's more fun than you'd think) and picking locks.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

DEF CON Training - Monday - 08:30-17:30 PDT

Title: Software Defined Radios 101 - Introduction to RF Hacking

Tags: DEF CON Training (Paid) (2-day) | DEF CON Training

When: Monday, Aug 10, 08:30 - 17:30 PDT

Where: LVCCW Level 3 W314 (Ham Radio Meeting) - [Map](#)

Description:

SpeakerBio: Richard Shmel

No BIO available



[Return to Index](#) - Add to Google

- ics [Calendar](#) file

DEF CON Training - Tuesday - 08:30-17:30 PDT

Title: Software Defined Radios 101 - Introduction to RF Hacking

Tags: DEF CON Training (Paid) (2-day) | DEF CON Training

When: Tuesday, Aug 11, 08:30 - 17:30 PDT

Where: LVCCW Level 3 W314 (Ham Radio Meeting) - [Map](#)

Description:

SpeakerBio: Richard Shmel

No BIO available



[Return to Index](#) - Add to Google

- ics [Calendar](#) file

Title: Software Quality in Electronic Voting

Tags: Voting Village | Creator Talk/Panel

When: Saturday, Aug 8, 10:30 - 10:59 PDT

Where: LVCCW Level 2 W220 (Voting Village) (Voting Village Talks) - [Map](#)

Description:

Casting a vote is the primary means by which citizens can influence their government. Following the passage of the Help America Vote Act (HAVA) in 2002, a surge in the use of electronic voting systems occurred. Although hand-marked paper is returning to use, the replacements in many jurisdictions for these aging electronic systems are also electronic. Given the serious nature of elections, electronic voting systems must be trustworthy, and their engineering must be held to rigorous standards.

We have had the opportunity, over the past eight years, to observe and analyze the use of electronic voting systems in the state of South Carolina. Our observations of such systems in the field have yielded serious usability, software, and hardware quality concerns, ranging from procedural errors resulting from poorly-designed systems, to system faults that ignore or miscount votes, to timestamp anomalies and malformed output. Given the importance of elections, and the inherent risk in the use of current electronic voting systems, we question the wisdom of using such systems until they are held to standards comparable to those used in other regulated, safety critical domains.

SpeakerBio: Duncan Buell

Duncan A. Buell is the Chair Emeritus of the NCR Chair in Computer Science and Engineering at the University of South Carolina. He holds a Ph. D. in mathematics from the University of Illinois, Chicago, and continues research interests in electronic voting, digital humanities, and text analysis. He was appointed in March 2019 to the Commission on Voter Registration and Elections of Richland County, South Carolina, resigning in March 2021 when he moved to Ohio. He taught computer science as a visitor at Denison University in Granville, Ohio, in academic years 2022-2023 and 2023-2024.

Dr. Buell has been analyzing election data, primarily from ES&S and Dominion systems, since 2010, including five complete biennials (2010-2018) from South Carolina, as well as data from AZ, GA, KS, NV, PA, and TX, and data from 2010 through 2024.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Sold Out - Agentic Threat Hunting: Building AI That Remembers What You Hunted

Tags: DEF CON Workshop | DEF CON Workshops

When: Friday, Aug 7, 09:00 - 12:59 PDT

Where: LVCCW Level 2 W233 (Workshops) - [Map](#)

Description:

Attendees hunt a supply chain compromise in real telemetry. Not a walkthrough - a hunt. A trojanized developer tool has been backdoored. The artifacts are seeded across a shared Splunk instance at layered difficulty: some obvious, some buried. Over four hours, attendees progress through the Five Levels of Agentic Hunting using the open-source Agentic Threat Hunting Framework (ATHF). Each maturity level unlocks new capabilities ,Â structure, searchability, AI research agents, and full agentic workflows ,Â that help them find what they couldn't find before. The first hunt is manual. By the last module, AI agents are surfacing hypotheses, identifying coverage gaps, and pointing hunters toward artifacts they missed. The human decides what to chase. The framework remembers what they found. This is not a tool demo. Attendees will make real analytical decisions, write real SPL queries, hit dead ends, and use AI agents to recover. They leave with a working ATHF workspace, documented hunts from a real investigation, and the experience of hunting with an agentic system.

SpeakerBio: Sydney "letswastetime" Marrone

Sydney Marrone is a threat hunter, SANS course author, co-founder of THOR Collective, author of the Agentic Threat Hunting Framework (ATHF), and co-author of the PEAK Threat Hunting Framework. She is passionate about helping defenders become better threat hunters by turning complex ideas into practical, repeatable techniques. Through open-source research, workshops, and community-driven projects, Sydney builds frameworks and resources that make hunting more structured, collaborative, and effective. Outside of work, she writes for THOR Collective Dispatch, lifts weights, and makes cyber-inspired music with AI.

--

Sydney Marrone is a threat hunter, cybersecurity professional, co-founder of THOR Collective, author of the Agentic Threat Hunting Framework, and co-author of the PEAK Threat Hunting Framework. She is passionate about making security knowledge accessible and actionable through hands-on research, open-source collaboration, and community-driven projects like HEARTH (Hunting Exchange And Research Threat Hub). Sydney creates resources, leads workshops, and shares insights that spark curiosity and empower defenders. Outside of work, she writes for THOR Collective Dispatch, lifts weights, and makes cyber-themed music using AI to blend creativity and hacker culture.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

DEF CON Workshops - (Sold Out) - Friday - 14:00-17:59 PDT

Title: Sold Out - All About Stoopie InfoStealers: Malware Analysis for Understanding, Custom Coding for True Understanding!

Tags: DEF CON Workshop | DEF CON Workshops

When: Friday, Aug 7, 14:00 - 17:59 PDT

Where: LVCCW Level 2 W231 (Workshops) - [Map](#)

Description:

Infostealers suck. We all know that. We don't like them. We want you to learn all that you can about them to help thwart the ongoing, ever-evolving threat. On that note, current infostealers are largely rule-based and path-driven, targeting known browser stores and wallets with noisy exfiltration methods. This four-hour workshop, led by Ryan Chapman and Aaron Rosenmund, moves beyond basic comprehension via observation to explore the evolution of precision-based malware. Students will utilize a live, on-demand lab environment to perform deep malware analysis using Ghidra to understand how current stealers operate.

The session then transitions from analysis to creation, where attendees code, compile, and re-build their own "evolved" stealers. We replace static file targeting with in-memory relevance models and trade obvious HTTPS exfiltration for stealthy timing and protocol-native patterns. This hands-on, kinesthetic experience focuses on building a custom arsenal from the ground up. Participants will learn to enhance their tools with behavioral stealth, transitioning from identifying "stoopie" patterns to implementing advanced, AI-driven tradecraft and custom red team tool operations.

You won't just learn how what an infostealer is. You'll learn how they operated end-to-end. Join us :).

Speakers: Ryan "@rj_chap" Chapman, Aaron "Ironical" Rosenmund

SpeakerBio: Ryan "@rj_chap" Chapman

Ryan Chapman is the author of SANS, FOR528: Ransomware and Cyber Extortion, course, teaches SANS, FOR610: Reverse Engineering Malware, course, and works as a threat hunter @ \$dayJob. Ryan has a passion for life-long learning, loves to teach people about ransomware-related attacks, and enjoys pulling apart malware. He has presented workshops at DEF CON and other conferences in the past and knows how to create a step-by-step instruction set to maximize hands-on learning.

SpeakerBio: Aaron "Ironical" Rosenmund

Aaron Rosenmund is an accomplished cybersecurity professional with extensive experience in various leadership roles across multiple organizations. Currently serving as the Managing Director of Tradecraft and Programs at OnDefend since September 2024, Aaron also holds a position at the National Guard Bureau as Staff Lead for the Cyber Shield Red Team, demonstrating a commitment to enhancing cybersecurity defenses. With a background that includes significant roles at Pluralsight, where responsibilities spanned content strategy and security skills development, and the Florida Air National Guard as a Lead Cyber Operator focused on defensive operations, Aaron has developed a comprehensive skill set in threat emulation, cyber system operations, and training. Additionally, past leadership positions as CEO at Aestus Industries and Vice President at Concrete Surface Innovations underscore strong management capabilities and operational expertise. Aaron holds multiple degrees in technology and cybersecurity from respected institutions, underscoring a solid educational foundation in this field.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

DEF CON Workshops - (Sold Out) - Sunday - 09:00-12:59 PDT

Title: Sold Out - Attacking Cloud APIs from the IoT Edge

Tags: DEF CON Workshop | DEF CON Workshops

When: Sunday, Aug 9, 09:00 - 12:59 PDT

Where: LVCCW Level 2 W222 (Workshops) - [Map](#)

Description:

This course covers attacking the cloud REST APIs and IoT provider (cloud customer responsibility) configurations to demonstrate data exfiltration, remote code execution, and lateral movement. Hands-on experience with using an already compromised, simulated IoT device as well as navigating pen testing (fuzzing) of the common protocols (i.e. MQTT, HTTP) will be covered.

Workshop goal Teach students practical, repeatable techniques to observe, extract, and abuse cloud API credentials and logic from the vantage of a compromised IoT device. Students will leave able to enumerate device, cloud flows, extract tokens, fuzz REST/MQTT endpoints, and demonstrate controlled lateral movement inside an isolated cloud tenant.

SpeakerBio: Rodney "BenevolentWorm" Beede

Rodney is an offensive security red team pen tester. He has specialized in cloud, web, and IoT security for over 18 years. He has spoken at multiple conferences (BSides, Def Con, Black Hat) on topics ranging from cloud security engineering to IoT device hacking. Rodney has been accredited with multiple CVEs for web vulnerabilities in products such as Wi-Fi hardware and security appliances. He started his career in enterprise web application software development but shifted to the security industry with this master's thesis research project "A Framework for Benevolent Computer Worms" 2012. Website: <https://www.rodneybeede.com/curriculum%20vitae/bio.html>

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

DEF CON Workshops - (Sold Out) - Friday - 09:00-12:59 PDT

Title: Sold Out - AWS Cloud Security 101: From IAM Misconfigurations to Account Takeover

Tags: DEF CON Workshop | DEF CON Workshops

When: Friday, Aug 7, 09:00 - 12:59 PDT

Where: LVCCW Level 2 W228 (Workshops) - [Map](#)

Description:

The shortest path from a marketing-site SSRF to production root often runs through AWS, and most defenders can,Äôt see it happening. This workshop teaches you to walk that path yourself.

Working whitebox in provided lab accounts, you,Äöll move through eight hands-on modules: reading IAM policies for privilege escalation gadgets, turning a single SSRF into a working CLI session via IMDS, abusing cross-account trust, exploiting resource policies across S3/KMS/Lambda, compromising serverless functions, and evading CloudTrail. The workshop closes with a full-chain challenge: build a Python exploit that goes from external SSRF to administrative access in one script.

Prerequisites: Basic AWS familiarity (console + CLI), comfort reading JSON policies, Python. Bring a laptop with AWS CLI v2 and Python 3.10+ installed. No prior offensive cloud experience required.

Speakers: zeta, Rafa "bane" Gutierrez

SpeakerBio: zeta

zeta is an internet plumber and computer toucher. he spends his days reading IAM policies and his nights wondering why anyone wrote them that way.

SpeakerBio: Rafa "bane" Gutierrez

"Rafael (bane) is the founder of Secure Origin, where he helps organizations doing public-interest work improve their security, infrastructure, and operational resilience. His work spans vulnerability research, security architecture, detection engineering, adversary emulation, infrastructure operations, and targeted technical engagements.

He is also a researcher and technical lead for The Southlander, a local Los Angeles newsroom. He volunteers with Lucy Parsons Lab and conducts independent research on surveillance technology, supporting reporting on how these systems affect journalists, activists, and local communities."

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

DEF CON Workshops - (Sold Out) - Friday - 14:00-17:59 PDT

Title: Sold Out - AWS Principal Threat Hunting: Behavioral Baselineing for Malicious Activity

Tags: DEF CON Workshop | DEF CON Workshops

When: Friday, Aug 7, 14:00 - 17:59 PDT

Where: LVCCW Level 2 W228 (Workshops) - [Map](#)

Description:

Cloud security encounters attacks that elude standard detection. In AWS, unauthorized access keys are a common cause of breaches. The vastness of AWS, over 450 services and 20,000 API actions, complicates threat visibility and exposes gaps in traditional tools.

This workshop empowers participants with direct, hands-on experience using the AWS Threat Hunter tool to improve threat detection. Attendees will focus on building behavioral baselines and leveraging data-driven analysis to detect subtle AWS principal anomalies, enabling more precise detection than traditional event monitoring.

Attendees will move beyond standard techniques by building multi-stage detection pipelines that create individualized baselines for each IAM principal and systematically flag personalized deviations, linking outliers directly to risks.

SpeakerBio: Rodrigo "Sp0oKeR" Montoro

Rodrigo Montoro is the CTO at Clavis Security, bringing over 25 years of leadership and technical expertise to the information technology and cybersecurity landscape. Throughout his career, Rodrigo has been a pioneer in open-source security, specializing in incident detection, response, and Cloud Security. A two-time patented inventor, he holds proprietary technologies for detecting malicious digital documents and analyzing malicious HTTP traffic. With a resume that includes key research roles at Tenchi Security, Apura, Tempest, Sucuri, and SpiderLabs, Rodrigo is a globally recognized authority who frequently speaks at elite conferences such as DEF CON Workshops (2023), DEF CON Cloud Village (3x), Black Hat Brazil Summit, SANS (DFIR, SIEM Summit, CloudSecNext), Source (Boston and Seattle), Toorcon (San Diego), Sector Canada (6x), and BSidesLV.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Sold Out - Battle-Tested Broadcasts: RF Insights From Ukraine

Tags: DEF CON Workshop | DEF CON Workshops

When: Saturday, Aug 8, 09:00 - 12:59 PDT

Where: LVCCW Level 2 W233 (Workshops) - [Map](#)

Description:

Every wireless thing in your life is broadcasting. The question is who's listening ,Â and what they can do with it. Battle-Tested Broadcasts is a four-hour, hands-on workshop on RF detection and direction finding, framed by the most demanding live laboratory in the world for these techniques: the Ukrainian frontline. We start with universal foundations ,Â frequency, modulation, antennas, what your SDR can and can't see ,Â and pivot into where neural-time RF detection becomes existential: drones. A pilot powers up an FPV controller thirty seconds before impact. Pure RF detection is often the only sensor in the chain that catches the threat before the drone leaves the ground. We cover what's actually in the air across a contested battlefield slice ,Â controllers, video downlinks, telemetry beacons, battlefield comms, GNSS, and the increasingly exotic bands operators are pushing into to dodge electronic warfare. We dissect the honest limits of common off-the-shelf SDR tooling, and the ways adversaries already evade pure RF detection: from fiber-optic and autonomous drones to wired front-line networks, frequency hopping, and out-of-scan spectrum. Attendees solder and flash a Signal Compass ,Â a pocket ESP32 signal detector with directional bearing. Rotating lab stations cover passive scanning, fingerprinting, direction findi

SpeakerBio: Preston Zen

Preston Zen , the original creator of 1337sheets.com, OSCE3 certified, now leading Kaizen Labs out of a Japan / Ukraine hybrid office. Software, hardware, and cybersecurity background. Volunteering in Ukraine since 2022 with NGOs including Dronarnia, BeeTA, American Made Freedom, and Shield of Freedom on drone systems, RF detection, EW countermeasures, and humanitarian logistics. DEFCON regular since DC25 and a Hac-Man CTF contributor for the past three years. He's shipped more boards than he's counted, and has spent enough time near the Ukrainian frontline to have strong opinions about which detection tools actually work when the noise floor is on fire.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

DEF CON Workshops - (Sold Out) - Saturday - 14:00-17:59 PDT

Title: Sold Out - Building Agentic Reverse Engineering "Skills"

Tags: DEF CON Workshop | DEF CON Workshops

When: Saturday, Aug 8, 14:00 - 17:59 PDT

Where: LVCCW Level 2 W231 (Workshops) - [Map](#)

Description:

Agentic reverse engineering blends interactive binary analysis with autonomous agent workflows. Building on workshops at REcon and DEF CON Singapore, this session introduces Agent Skills, structured bundles of instructions, scripts, and resources that coding agents discover and execute. Skills enable multi-step RE tasks with high accuracy and minimal prompting via workflow capture and progressive disclosure.

Participants learn how coding agents operate through iterative loops (generate, execute, inspect, refine) and how Skills plug into these loops. The workshop is hands-on: attendees build a multi-platform driver-analysis Skill automating IOCTL enumeration, dispatch-flow analysis (Windows IRPs, Linux file ops, macOS IOKit), code-flow analysis, and workflow capture. A capstone challenge has participants build a second Skill from scratch.

Supports Claude Code, OpenCode, Mistral Vibe, and pi. The instructor provides LLM inference for all attendees, so no paid API keys are required. Students may also use free inference tiers from OpenCode or similar providers.

Attendees leave with practical experience to implement agentic RE Skills in their own workflows. Basic familiarity with RE concepts and a laptop with a coding agent installed is all that is needed.

SpeakerBio: John "clearbluejar" McIntosh

John McIntosh (@clearbluejar) is a security researcher and founder of ClearSecLabs, specializing in reverse engineering, vulnerability research, and AI-assisted binary analysis. He is the author of ghidriff, an open-source Ghidra-based binary diffing engine, and pyghidra-mcp, a headless Ghidra MCP server enabling LLM-driven, project-wide, multi-binary reverse engineering workflows. An active contributor to the Agent Skills ecosystem, John bridges deterministic analysis with AI-driven reasoning to accelerate vulnerability research. He has delivered training and workshops at DEF CON, Black Hat, REcon, Ringzer0, 44CON, Objective by the Sea, and Insomni'hack, covering topics from practical Windows reverse engineering to building private local LLM RE stacks. His recent work includes the "Agentic RE" training at DEF CON Singapore 2026, the MCP Ghidra workshop at REcon 2025, and the "Supercharging Ghidra" LLM workshop at Ringzer0 COUNTERMEASURE 2025. With over a decade of offensive security experience, John publishes detailed research on reversing CVEs, building RE tooling, and agentic patch diffing at clearbluejar.github.io. His teaching emphasizes reproducibility, progressive skill-building, and contributor empowerment.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

DEF CON Workshops - (Sold Out) - Sunday - 09:00-12:59 PDT

Title: Sold Out - Building your own hardware hacking kit to Pentest Bluetooth, WIFI, and more.

Tags: DEF CON Workshop | DEF CON Workshops

When: Sunday, Aug 9, 09:00 - 12:59 PDT

Where: LVCCW Level 2 W225 (Workshops) - [Map](#)

Description:

You will receive a free hardware kit, documentation, and class introduction to the same hardware configuration used by hundreds of hacking hardware tools as their main core. We will cover Wifi Hacking on both 2 and 5ghz, Bluetooth hacking, packet capture, Flipper interface (bring yours if you have one), Sensor integration (also included), Mesh networking, point to point communications and more. Requirements: Laptop, Fully charged, USB-A interface, Windows OS (we will discuss MAC and Linux, but you will need to have knowledge and permissions to install tools). You can attend without above and still get kit, but it will not be hands on. All information will be published after the workshop if you don't have a laptop. You will get a modern ESP32, Sensor, breadboard, USB cable, wires and more during the workshop.

SpeakerBio: Dallas

Dallas has been involved in hacking since early teens, which translates to sometime in the 80's. Mentored by Satellite and Ham hackers, has been involved in a few organizations including all levels of government, 3 letter agencies, serving as Chief security officer, CISO, and technical manager of multiple world-wide organizations. Banking, Energy, Space, Telecom, Government and manufacturing. Elected, re-elected, served and got the trophy. OG Considered an expert in Pen testing, variety of related and unrelated technology ,À occasionally serving 15+ years as a Defcon security goon, and around 10 for B-sides organizations. Alexa Park being his first Defcon. Mostly bored, but thinks AI is kind of fun and enjoys giving back to the community. Doing his best to not get arrested, and share knowledge with those interested in seeking it.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Sold Out - CI/CD Weaponization: Build It, Deploy It, Own It

Tags: DEF CON Workshop | DEF CON Workshops

When: Sunday, Aug 9, 09:00 - 12:59 PDT

Where: LVCCW Level 2 W230 (Workshops) - [Map](#)

Description:

GitHub Actions has become the de facto automation layer for modern software, and the de facto attack surface. In 2025, a single compromised Action leaked secrets across 23,000 repositories. One year later, the TeamPCP group ran the same playbook at scale by compromising Trivy's actions. Different victims, same root cause: a CI/CD pipeline that trusted what it shouldn't.

In this hands-on workshop, participants will build a complete end-to-end attack chain in a controlled lab environment, emulating adversary TTPs observed in recent GitHub Actions breaches. From initial access through malicious workflow manipulation to secret exfiltration, each phase is paired with detection and analysis techniques to bridge offensive and defensive perspectives.

Whether you're on a red or purple team looking to simulate attacker behavior, or part of a blue team (AppSec or DevSecOps) aiming to harden CI/CD pipelines, this workshop delivers practical, real-world skills grounded in today,Ãs evolving threat landscape.

Speakers: Ricardo Sanchez, Daniel Malvaceda

SpeakerBio: Ricardo Sanchez

Ricardo Sanchez is an accomplished cybersecurity professional with a passion for empowering others through knowledge sharing. He has built his career designing and implementing innovative technology strategies for threat intelligence, detection engineering, and threat hunting to combat evolving cyber threats. Currently, Ricardo leads the Application Security (AppSec) practice at a leading insurance company in Peru, where he works closely with DevSecOps teams to enhance security across the software development lifecycle (SDLC) and supply chain. Committed to lifelong learning, Ricardo thrives on analyzing malware and staying at the forefront of cybersecurity advancements.

SpeakerBio: Daniel Malvaceda

Daniel Malvaceda is a security architect who spends most of his time figuring out how CI/CD pipelines and supply chains actually fail, then writes it up so others don't have to learn it the hard way. Lately he's also poking at AI/LLM agents, since pipelines aren't the only thing shipping untrusted code anymore. He co-founded pipebreach.com, where real-world supply chain attacks get reproduced, dissected, and written up for everyone else. He also co-organizes the DevSecOps village at Ekoparty (Argentina and Miami), and has dragged these same topics to stages at Ekoparty, DevOps Days, and 8.8 Security Conference. If a pipeline can be weaponized, he wants to know about it first.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Sold Out - Creating Shellcode for Hackers

Tags: DEF CON Workshop | DEF CON Workshops

When: Sunday, Aug 9, 09:00 - 12:59 PDT

Where: LVCCW Level 2 W232 (Workshops) - [Map](#)

Description:

Creating shellcode is for the brave! This workshop takes a modern approach to the time-honored tradition of Windows shellcode creation. Intended for those with intermediate to advanced knowledge, we will refresh x86 assembly and cover Windows internals.

You will create Win32/WoW64 shellcode with NASM before moving onto intermediate, multi-API shellcode. Along the way, we will cover GetPC, position independence, bad characters, calling conventions, stack discipline, manual API resolution through the PEB/TEB, export walking, name/hash-based resolution, strings, and passing handles or pointers between calls.

For evasion, we will explore manual/automated encoding techniques, making our shellcode self-modifying. We will also cover advanced techniques, including direct Windows syscalls with ShellWasp. You will learn Windows structures, native API parameter handling, and creating persistence with syscalls. Expect to be made privy to many shellcoding tips and tricks to bring out the best in your shellcode.

By the end, you'll be able to: Create Windows shellcode using NASM; launch and debug it; resolve and chain WinAPIs by name or hash; obfuscate and encode shellcode; integrate direct syscalls with ShellWasp.

Prep: Study x86 assembly and basic Windows debugging. A VM will be provided. Required: modern PC (Intel) / VM

Speakers: Bramwell "Bw3ll" Brizendine, Austin "quantumite" Norby, Micah Flack

SpeakerBio: Bramwell "Bw3ll" Brizendine

Dr. Bramwell Brizendine has a Ph.D. in Cyber Operations and is the Director of the VERONA Lab. Bramwell has regularly spoken at DEFCON and presented at all regional editions of Black Hat (USA, Europe, Asia, MEA), as well as at Hack in the Box Amsterdam, Virus Bulletin, and Wild West Hackin' Fest. Bramwell received a \$300,000 NSA research grant to create the SHAREM shellcode analysis framework, which brings unprecedented capabilities to shellcode analysis and \$500,000 as a 2025 DARPA YFA recipient for a PE file emulation framework. He has additionally authored ShellWasp, which facilitates using Windows syscalls in shellcode, as well as two code-reuse attack frameworks, ROP ROCKET and JOP ROCKET. Bramwell has previously taught undergraduate, master's, and Ph.D. courses on software exploitation, reverse engineering, offensive security, and malware analysis. He currently teaches cybersecurity courses at the University of Alabama in Huntsville.

SpeakerBio: Austin "quantumite" Norby

Dr. Austin Norby is a seasoned cybersecurity professional with over a decade of experience supporting the Department of Defense. He earned his bachelor's degrees in mathematics and computer science from the University of Minnesota, a master's degree from the Naval Postgraduate School, and a Doctorate in Cyber Operations from Dakota State University, specializing in anti-debugging techniques. Currently, Dr. Norby serves as the Director of Internal Research and Development at Bogart Associates, where he is responsible for spearheading the creation of advanced cybersecurity solutions for government use. His technical proficiencies include reverse engineering, malware analysis, and software engineering, with a strong focus on developing robust cyber capabilities in C, C++, Intel assembly, and Python.

SpeakerBio: Micah Flack

Micah Flack is a cybersecurity researcher at Idaho National Laboratory, where his work spans vulnerability research, firmware and hardware analysis, malware forensics, exploit development, and reverse engineering across multiple platforms and architectures. He is currently pursuing a Ph.D. in Cyber Operations at Dakota State University, with research interests rooted in applied cybersecurity, software exploitation, malware analysis, and shellcoding. Micah also holds both a Master's degree in Computer Science and a Bachelor's degree in Cyber Operations from DSU, where he was active in cybersecurity research and competitions. Micah brings a hands-on perspective from his varied experiences in working with assembly, payload development, embedded systems, and offensive security research.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Sold Out - Detecting and Analyzing Memory Only Malware with Volatility 3

Tags: DEF CON Workshop | DEF CON Workshops

When: Saturday, Aug 8, 09:00 - 12:59 PDT

Where: LVCCW Level 2 W232 (Workshops) - [Map](#)

Description:

Memory-only malware is now commonly used by threat actors ranging from criminal organizations to ransomware operators to APT groups. To detect such malware, memory forensics, which is the examination of a system's volatile memory (RAM), must be performed. Volatility 3 is the latest version of the Volatility Memory Analysis framework and is the most widely used open-source framework for memory forensics. In this workshop, students will learn how to use Volatility 3 to detect the most sophisticated malware techniques found in the wild. This learning will occur through a mixture of lectures, live demos, and extensive hands-on labs where students analyze memory samples infected with real malware. While students work through labs, instructors walk to each student's station to ensure they are progressing. An instructor also walks through each lab live upon completion, and students are given a 35+ page lab guide that contains all the scenarios, questions, and detailed answers. Students can later use the course slides and lab guide to practice as well as to guide real-world investigations. The workshop's instructors are core Volatility developers who have made significant contributions to the project. By attending this workshop, students will gain deep knowledge and hands-on experience analyzing memory-only malware.

Speakers: Andrew Case, Pierre "Abyss Watcher" Breton, David McDonald

SpeakerBio: Andrew Case

Andrew Case is the Director of Research at Volexity and has significant experience in incident response handling, digital forensics, and malware analysis. Case is a core developer of Volatility, the most widely used open-source memory forensics framework, and a co-author of the highly popular and technical forensics analysis book "The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory." Case has spoken at many industry conferences, including DEF CON, Black Hat, RSA, DFRWS, SecTor, BSides*, and OMFw.

SpeakerBio: Pierre "Abyss Watcher" Breton

Pierre (Abyss Watcher) Breton is a researcher at Volexity, holding a Master of Science in Cybersecurity, specializing in digital forensics, malware analysis and detection engineering. He is a primary contributor to Volatility, the most widely used open-source memory forensics framework. Breton has demonstrated a great ability to assist the incident response community by developing innovative capabilities and resources. He conveys his passion through the organization of CTF events and training sessions that showcase both accessible and challenging topics.

SpeakerBio: David McDonald

David McDonald is a researcher and software engineer with 5 years of digital forensics R&D experience. His passion for this field began with his involvement in the University of New Orleans CTF team, as well as through his time as a Systems Programming teaching assistant. After over two years of digital forensics research and development on Cellebrite's computer forensics team, he joined Volexity's Volcano team, where he now works to develop next-generation memory analysis solutions. He believes deeply in sharing knowledge and helping others discover their abilities and interests through their own journeys in cybersecurity, and strives to pay forward the benefits of the mentorship that has opened so many doors for him.



DEF CON Workshops - (Sold Out) - Friday - 14:00-17:59 PDT

Title: Sold Out - Embedded Computing Tools for Wireless Hardware Hacking

Tags: DEF CON Workshop | DEF CON Workshops

When: Friday, Aug 7, 14:00 - 17:59 PDT

Where: LVCCW Level 2 W233 (Workshops) - [Map](#)

Description:

Hands-on exploration of embedded hardware tools implementing multiple wireless communication standards. Experiment with Wi-Fi wireless local area network (WLAN) technology and Bluetooth personal area network (PAN) technology. Stream audio to and from a variety of endpoints. Configure a Nordic nRF52 Bluetooth sniffer to capture and analyze wireless communications using Wireshark. Examine the design and manufacture of an exclusive dual-core embedded hardware target supporting both Wi-Fi and Bluetooth. Leverage the target to experiment with microcontroller-based wireless hardware hacking. Practice both sinking and sourcing Bluetooth Audio streams into and out of the hardware target. Capture Wi-Fi packets using onto the hardware target for transfer to Wireshark for analysis. Perform example security exploits and countermeasures using embedded wireless hardware tools.

PLEASE NOTE: This workshop requires purchasing the necessary hardware tools. A link to complete the purchase of \$60 will be provided upon registration for the workshop. The purchased kits will be distributed during the workshop.

SpeakerBio: Joseph Long

Joseph Long has been tinkering, designing, and hacking electronic systems for about forty years. He is the founder of HackerBoxes.com, the monthly subscription box service for electronics, cybersecurity, and hacker culture. Joseph is a licensed professional engineer and patent attorney who loves to teach electrical engineering and computer science topics.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

DEF CON Workshops - (Sold Out) - Saturday - 14:00-17:59 PDT

Title: Sold Out - Entra ID Persistence - Because Passwords Were Never the Problem

Tags: DEF CON Workshop | DEF CON Workshops

When: Saturday, Aug 8, 14:00 - 17:59 PDT

Where: LVCCW Level 2 W228 (Workshops) - [Map](#)

Description:

Modern enterprise security has shifted from network boundaries to identity, making Microsoft Entra ID a critical control plane and a prime target for persistence. While credential theft remains common, sophisticated attackers increasingly establish long-term access through identity-layer backdoors that survive password resets and evade traditional monitoring.

We will explore how attackers achieve durable persistence in Microsoft Entra ID by abusing service principals, federated identities, passwordless authentication methods, and device trust relationships. The session highlights techniques that remain effective even after common remediation actions like credential rotation and MFA enforcement. Through guided, hands-on scenarios, participants will simulate these identity-layer persistence techniques and understand their real-world impact demonstrating how adversaries integrate into legitimate identity workflows to maintain covert, long-term access without raising immediate suspicion.

Participants will step into the role of an adversary and explore how persistence is established and maintained inside Microsoft Entra ID. Rather than focusing on theory, this workshop breaks down real-world attack paths used to retain access beyond initial compromise highlighting techniques that survive password resets, MFA enforcement

Speakers: Raunak "Trouble1" Parmar, Chirag "3xpl01tc0d3r" Savla

SpeakerBio: Raunak "Trouble1" Parmar

Raunak Parmar works as a senior cloud security engineer at White Knight Labs with 6+ years of experience. His areas of interest include web penetration testing, Azure/AWS security, source code review, scripting, and development. He enjoys researching new attack methodologies and creating open-source tools that can be used during cloud red team activities. He has worked extensively on Azure and AWS and is the author of Vajra, AzDevRecon and MsCodePhish. He has spoken at multiple respected security conferences like Black Hat, Defcon, Nullcon, RootCon, HackspaceCon, NorthSec, LeHack, etc and also at local meetups.

SpeakerBio: Chirag "3xpl01tc0d3r" Savla

Chirag Savla is a Cyber Security professional with 10+ years of experience. His areas of interest include penetration testing, red teaming, azure and active directory security, and post-exploitation research. He prefers to create open-source tools and explore new attack methodologies in his leisure. He has worked extensively on Azure, Active Directory attacks, defense, and bypassing detection mechanisms. He is an author of multiple Open Source tools such as Process Injection, Callidus, etc. He has presented at multiple conferences and local meetups and has trained people in international conferences like Blackhat, BSides Milano, Wild West Hackin, Aô Fest.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

DEF CON Workshops - (Sold Out) - Saturday - 09:00-12:59 PDT

Title: Sold Out - Explore the Windows instrumentation callback

Tags: DEF CON Workshop | DEF CON Workshops

When: Saturday, Aug 8, 09:00 - 12:59 PDT

Where: LVCCW Level 2 W225 (Workshops) - [Map](#)

Description:

The Nirvana Debug is a type of instrumentation callback existing since Windows 7. This workshop idea is to see how this feature can be weaponized in order to either: - Hijack execution flow - Perform process injection - Perform sleep obfuscation for C2 beacon

During this workshop, you will learn the main principle of Nirvana Debugging, and try to weaponize it. Some debugging, reverse and coding will be needed in order to create a new malware that will evade classic EDR solutions.

SpeakerBio: Yoann "OtterHacker" DEQUEKER

Yoann Dequeker (@OtterHacker) is a red team operator at Wavestone entitle with OSCP and CRT0 certification. Aside from his RedTeam engagements and his contributions to public projects such as Impacket, he spends time working on Malware Developpement to ease beacon deployment and EDR bypass during engagements and is currently developing a fully custom C2.

His research leads him to present his results on several conferences such as LeHack (Paris), Insomni'hack (Swiss) or even through a 4-hour malware workshop at Defcon31,32 and 33 (Las Vegas). All along the year, he publishes several white papers on the techniques he discovered or upgraded and the vulnerabilities he found on public products.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

DEF CON Workshops - (Sold Out) - Saturday - 14:00-17:59 PDT

Title: Sold Out - From Prompt to PWN: Exploiting LLM Powered Web Applications with OWASP Techniques

Tags: DEF CON Workshop | DEF CON Workshops

When: Saturday, Aug 8, 14:00 - 17:59 PDT

Where: LVCCW Level 2 W229 (Workshops) - [Map](#)

Description:

This hands-on workshop explores the offensive security of AI-powered applications where Large Language Models connect to real tools via MCP (Model Context Protocol) servers. Over four hours, participants attack 11 purpose-built AI agents across 9 exercises, exploiting vulnerabilities mapped to the OWASP Top 10 for LLM Applications 2025.

You will perform prompt injection (direct and indirect via RAG poisoning), force AI agents to generate malicious SQL/NoSQL queries through MCP tool interfaces, chain path traversal and SSRF through tool-calling parameters, abuse excessive agency via MCP-exposed CRUD operations, trigger stored XSS through LLM output, and achieve remote code execution via a poisoned supply chain, all through natural language conversation.

This workshop is ideal for red teamers, penetration testers, security engineers, and developers building with LLMs. No prior AI or ML experience is required; every technique is demonstrated before the hands-on lab. Just bring a laptop with a browser.

You walk away with practical experience exploiting 93 attack objectives against live LLM agents, a clear understanding of how traditional web vulnerabilities are amplified through AI tool-calling architectures, and the instincts to spot these risks in your own AI deployments.

SpeakerBio: Abhinav Verma

Abhinav Verma is a Senior Staff Security Engineer at Intuit Inc. with 15+ years of experience across AI security, offensive security, red teaming, product security, and security operations. He currently leads AI security architecture reviews, AI penetration testing, and vulnerability management programs, with a focus on AI security, AI threat modeling, and securing large-scale cloud platforms.

Over the course of his career at Intuit, he has built security automation, scaled continuous security scanning across thousands of assets, led secure design reviews for platforms serving millions of customers, and developed secure coding programs that have helped thousands of engineers shift security left. Abhinav was formerly an independent security researcher and has identified and reported vulnerabilities in numerous major online services and technology companies.

He holds certifications including OSEP, OSCP, OSWP, GWAPT and CEH. Outside of work, Abhinav is a passionate gamer, a trained chef, an avid camper, and a mentor to aspiring offensive security practitioners.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

DEF CON Workshops - (Sold Out) - Saturday - 09:00-12:59 PDT

Title: Sold Out - HackTheCloud26: Chaining Cloud Misconfigurations to Compromise Infrastructure

Tags: DEF CON Workshop | DEF CON Workshops

When: Saturday, Aug 8, 09:00 - 12:59 PDT

Where: LVCCW Level 2 W230 (Workshops) - [Map](#)

Description:

HackTheCloud25 CTF Manager is an automated orchestration framework designed for the management of cloud cybersecurity challenges. It enables the deployment of intentionally vulnerable laboratories across AWS, Azure, and GCP using Terraform as the underlying Infrastructure-as-Code engine. The solution centralizes challenge definitions via YAML files, managing complex dependencies, dynamic variables, and resource outputs through a unified command-line interface (CLI) to list, deploy, destroy, and monitor resources in a controlled environment.

Furthermore, the framework incorporates environment validation, automated credential detection, detailed event logging, and support for reusable configurations, ensuring high scalability and traceability for complex attack scenarios. Collectively, the CTF Manager provides a reproducible and extensible approach to orchestrating practical cloud security exercises for educational purposes, streamlining the creation, operation, and maintenance of vulnerable infrastructures within dedicated testing environments.

SpeakerBio: HackeMate

HackeMate is the host of the YouTube channel under the same name, where the creator, an Offensive Cybersecurity Engineer, shares their expertise in ethical hacking, as well as offensive and defensive security. With over 30,000 subscribers engaged in the world of cybersecurity, they have established themselves as a key figure in the community through challenges, technical analyses, and hands-on demonstrations. Professionally, HackeMate holds Red Team certifications such as the eLearnSecurity Junior Penetration Tester (eJPT) and Web Penetration Tester (eWPT), along with Blue Team certifications like Microsoft Azure Fundamentals (AZ-900) and Microsoft Security, Compliance, and Identity Fundamentals (SC-900). They are also a Google Product Expert for Google Drive, contributing their knowledge in cloud security and optimization.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

DEF CON Workshops - (Sold Out) - Saturday - 14:00-17:59 PDT

Title: Sold Out - Hands-on DuckyScript: An Introduction to HID Attack Tools with O.MG Devices

Tags: DEF CON Workshop | DEF CON Workshops

When: Saturday, Aug 8, 14:00 - 17:59 PDT

Where: LVCCW Level 2 W222 (Workshops) - [Map](#)

Description:

"Don't plug in devices you don't trust." It's one of the most repeated pieces of security advice in the industry. What actually happens when a malicious USB device is plugged in? How does it work? This hands-on, four-hour workshop answers those questions by putting the tools directly in attendees' hands. Using O.MG Devices and the DuckyScript v3 scripting language, participants will learn the fundamentals of Human Interface Device (HID) attacks from the ground up. Starting from USB protocol basics all the way through real payload design, delivery strategy, and advanced techniques including wireless triggering, C2 integration, and air-gapped exfiltration (using HIDX StealthLink). The class is beginner-friendly and builds progressively: no prior red teaming experience is required. Only a DuckyScript v3 device is required. Attendees will leave with working scripts, a framework for payload design, and an understanding of what attackers and defenders need to look for. We will cover OpSec, detection (and evasion), and how accessibility-first design thinking can make both attackers and defenders more effective.

Speakers: wasabi, Ø1, Tokugero

SpeakerBio: wasabi

wasabi is a researcher, tinkerer, and professor of cybersecurity whose work spans IoT and embedded systems, cloud infrastructure, and offensive tooling. Their research focuses on uncovering systemic weaknesses across modern embedded environments, with an emphasis on practical exploitation and defensive resilience. When not tinkering, wasabi spends most of his time outdoors in nature.

SpeakerBio: Ø1

Ø1 is a seasoned offensive security professional who turned a lifelong passion into a dynamic career. Beginning as a machine operator, he transitioned into the world of cybersecurity, where he has since traveled globally, conducting and leading numerous penetration tests and red team engagements. With a wealth of hands-on experience, he excels at identifying vulnerabilities and strengthening defenses for organizations worldwide. In 2022, he joined the O.MG team, balancing this role alongside his primary job to contribute to product testing, documentation, tooling, and customer support. Beyond his professional pursuits, √ø1 is a devoted cat father with a love for guns, cars, BBQ, and gardening.

SpeakerBio: Tokugero

Tokugero is a Site Reliability Engineer and Cloud Architect focused on incident response, operations engineering, and running resilient infrastructure at scale. He works across the full ops stack ,Ä from system design and automation to the messy realities of keeping production healthy.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

DEF CON Workshops - (Sold Out) - Friday - 09:00-12:59 PDT

Title: Sold Out - Hands-on IoT firmware extraction and flash forensics

Tags: DEF CON Workshop | DEF CON Workshops

When: Friday, Aug 7, 09:00 - 12:59 PDT

Where: LVCCW Level 2 W225 (Workshops) - [Map](#)

Description:

Did you ever wanted to hack an IoT device but did not know how to start? Having UART is nice, but does not help in many cases.

For a complete analysis of an IoT device, it is required to look at the firmware itself. In most cases this means that the firmware, data or encryption keys need to be extracted from the device memory. Many researchers are hesitant to do that as there is a high risk of destroying the device or leaving it in an inoperable state. In this workshop we will look at different flash memory types (EEPROM, SPI flash, NAND flash, eMMC flash) and how to extract the information from them.

We will show that you do not need very expensive hardware to archive your goal and that it is not as complicated as everyone believes. See which tools might be useful for your own lab!

Participants will have the opportunity to work in groups and being provided different kinds of IoT devices (e.g. smart speakers). After a tear-down, you can use different chip-off methods (e.g. Hot air, IR soldering) to remove the flash chip and read it out. Optionally, the tools re-ball and re-solder the IC will be available after the workshop. In the end, each team should have the data and a functional device again.

Bonus: If you brick the device, you can keep the parts as a souvenir or can wear them as badges.

Speakers:Dennis Giese,Braelynn Luedtke,Arnold Wey,Harsha Potu

SpeakerBio: Dennis Giese

Dennis Giese is a researcher with the focus on the security and privacy of IoT devices. While being interested in physical security and lockpicking, he enjoys applied research and reverse engineering malware and all kinds of devices. His most known projects are the documentation and hacking of various vacuum robots. He calls himself a "robot collector" and his current vacuum robot army consists of over 95 different models from various vendors. He talked about his research at the Chaos Communication Congress, REcon, HITCON, NULLCON, and DEFCON.

SpeakerBio: Braelynn Luedtke

Hacker and tomato farmer. Enjoys researching the security of anything that piques her curiosity. She has previously presented this research at conferences such as Chaos Communication Congress, HITCON and DEFCON.

SpeakerBio: Arnold Wey

Arnold Wey is an electronics security researcher. His recent work includes security testing of virtual GPU implementations, robot arm communication protocols, and repurposing a 3D printer for fault injection research.

SpeakerBio: Harsha Potu

Harsha has been taking things apart since he could get his hands on a screwdriver for fun and profit. Nowadays he is a cybersecurity researcher with a decade of experience in embedded security. He loves to reverse boards + firmware and regularly finds vulnerabilities at various layers of execution. Especially interested in breaking secure boot chain designs!



Title: Sold Out - Hecate: A Trivial UART Tool

Tags: DEF CON Workshop | DEF CON Workshops

When: Saturday, Aug 8, 09:00 - 12:59 PDT

Where: LVCCW Level 2 W231 (Workshops) - [Map](#)

Description:

Hecate is an open source UART implant framework designed to make common hardware hacking tasks easy with minimal code. It turns any CircuitPython microcontroller into a powerful, customizable UART implant.

In this workshop, you'll get to use all the core features of Hecate and see how they work against multiple target devices. We'll start hands-on by listening to a device's UART output, and then configuring Hecate to operate in standalone mode and log that UART data to a file. Once we've seen it in action, we'll step back for a bit of lecture about UART, what it's used for, and what we designed Hecate to be capable of. Armed with this knowledge, you'll dive into two more hands-on labs: a payload dropper that will playback a custom transaction and a simple detector that will signal an alert when it detects a pattern. We'll reconvene for a last bit of lecture on how to use some of Hecate's advanced features, before you dive into the final lab: implement a full implant-in-the-middle capable of modifying UART data in flight.

Hecate makes developing embedded implants trivial, while remaining flexible enough for advanced research and rapid prototyping. You'll walk away with hands-on experience using the Hecate framework and a working understanding of what's possible with UART interception, manipulation, and exploitation

Speakers:mx,Joe "SecurelyFitz" FitzPatrick,nyx

SpeakerBio: mx

Maxie is an erstwhile cloud infrastructure engineer, formerly an SRE at Google Cloud Platform and others. She came to the world of hardware hacking and embedded devices first as a pleasant escape from the quotidian indignities of working in the cloud, and she stayed for the addictive aroma of flux fumes. She enjoys making ill-advised expansions to her homelab and spending evenings at her local hackerspace in Portland, OR.

SpeakerBio: Joe "SecurelyFitz" FitzPatrick

Joe FitzPatrick (@securelyfitz) is a trainer and researcher at SecuringHardware.com with a personal mission to make all hardware devices at least a bit more secure. He builds tools like Tigard and Erebus, and teaches Applied Hardware Attacks trainings to help people break - and secure - their hardware devices. His actual superpower is the ability to instantly end awkward conversational pauses if you ask him about BSides Portland, the CTRL-H Hackerspace, or drone taco delivery at ToorCamp.

SpeakerBio: nyx

nyx is a Portland-based hacker, engineer, and self-described cyberpunk. As an unwilling participant in the late-capitalist, mass-surveillance dystopia, he is passionate about digital privacy, data self-custody, and running his own infra. While voiding warranties has long been one of his favorite pastimes, he has lately been fortunate enough to do it professionally as well.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Sold Out - ICS Hack 'n Track

Tags: DEF CON Workshop | DEF CON Workshops

When: Sunday, Aug 9, 09:00 - 12:59 PDT

Where: LVCCW Level 2 W231 (Workshops) - [Map](#)

Description:

OT attacks are often discussed but rarely demonstrated - in this workshop we use Caldera for OT to demonstrate realistic attack vectors for Distributed Control Systems used in power plants and other critical infrastructure, as well as how FOSS tools like Malcolm give defenders the information needed to detect blast radius and impacts.

Speakers: Pedro Cabrera, Hannes "hercules_hannes" Heck, Sam Miorelli, Jordan Sanchez

SpeakerBio: Pedro Cabrera

Pedro Cabrera is an OT cybersecurity professional and Omnivise Cybersecurity Solutions Architect at Siemens Energy. He specializes in industrial control systems and adversary simulation, focusing on bridging the gap between traditional IT security and operational technology through practical, real-world demonstrations. He has developed custom tooling to simulate PLC interactions and highlight detection challenges in OT environments. His work centers on improving visibility, strengthening defenses, and making complex security concepts more accessible.

SpeakerBio: Hannes "hercules_hannes" Heck

Hannes is an OT security practitioner currently completing a Bachelor's degree in Cybersecurity, with a thesis focused on Network Detection and Response systems including Malcolm. Active in the technology field since 2018, when he began a formal computer science apprenticeship, he has progressively deepened his specialization in cybersecurity and currently works at Siemens Energy in an OT Security role focused on solution architecture for industrial environments. He has presented technical topics in both academic and enterprise settings and brings direct hands-on experience with network traffic analysis, industrial control system design, and adversary emulation platforms to this workshop.

SpeakerBio: Sam Miorelli

Sam Miorelli is the Global Head of Innovation and Customer Success for Siemens Energy Omnivise Cybersecurity. By training he is a mechanical engineer and a lawyer. Prior to his involvement with OT cybersecurity, Sam was the primary lawyer for several billion dollars per year of energy and industrial automation transactions at Siemens worldwide.

SpeakerBio: Jordan Sanchez

Jordan Sanchez is a Cybersecurity Fellow at Siemens Energy, where he has spent three years doing R&D in OT and ICS security. Graduating from the University of Central Florida with a degree in Computer Science, he conducted undergraduate research on dependency downgrade vulnerabilities in the Android build system. Jordan is joining Amazon as a Security Engineer in September 2026.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Sold Out - Intro to Writing Windows Malware with Rust!

Tags: DEF CON Workshop | DEF CON Workshops

When: Saturday, Aug 8, 14:00 - 17:59 PDT

Where: LVCCW Level 2 W230 (Workshops) - [Map](#)

Description:

In the Information Security news space, we often hear about the cool malware and tools nation states and APTs develop. While there are many tools out there that "do the thing", have you ever wonder how it "does the thing"? Instead of just using tools and scripts that sound cool, why not make them?

Using the Rust programming language, you'll be taken step-by-step into building your own Windows malware! We'll break down the process and work our way into more complex tasks. From a simple, no-imports binary we'll slowly work into loading and executing Windows API functions without ever calling "LoadLibrary" or "GetProcAddress" while not touching a single Rust "std::*" function or importing any extra crates!

You'll be introduced into Windows concepts like the Process Environment Block (PEB), the Thread Environment Block (TEB) and how we can use them to our advantage! At the end of this workshop, you'll be able to build binaries without any imports while doing fun tricks like shellcode injection!

Some of the topics we'll touch on are:

- Assembly!
- Rust Allocators
- Windows Structs
- API Function Calls
- Binary File Inspection

Speakers: iDigitalFlame, Daniel Bravo

SpeakerBio: iDigitalFlame

iDigitalFlame is an experienced security researcher that uses his programming skills to expand his abilities and provide teams with the tools needed to complete any engagement. Outside of work, his passion for open source and knowledge sharing has led to the creation of many unique tools and resources. iDigitalFlame also uses his skills to help power many CTFs, including the ProsVJoes CTF at BSidesLV, where he leads the Red Team and provides the platform for Red operations. iDigitalFlame has spoken before at BSidesDE and BSidesLV about cool things learnt in his research like AV evasion or releases open source software like ThunderStorm, a custom C2 platform used in many CTFs he operates in.

SpeakerBio: Daniel Bravo

Daniel is a self-taught programmer who later earned a B.S. in Computer Science from the University of Maryland. He likes to understand how software works by decompiling binaries and reverse engineering APIs, whether they were meant to be understood or not. Daniel also enjoys working on geospatial projects and web scraping tools, particularly extracting and reconstructing data from mobile platforms. His other interests also include compiler theory, automated reasoning, and verification-aware languages.

DEF CON Workshops - (Sold Out) - Friday - 14:00-17:59 PDT

Title: Sold Out - Introduction to Malware Analysis

Tags: DEF CON Workshop | DEF CON Workshops

When: Friday, Aug 7, 14:00 - 17:59 PDT

Where: LVCCW Level 2 W232 (Workshops) - [Map](#)

Description:

Analyze malware to find indicators of compromise using static and dynamic techniques. We will analyze Windows executables at the binary level and modify them to cheat at games. We will examine both compiled code and DOTNET executables. We will also examine defenses to prevent memory-corruption attacks, including coding in Rust.

We will demonstrate the techniques and help attendees solve challenges. There are dozens of hands-on projects, with a running CTF scoreboard. Some of the projects are easy enough for beginners, and others will challenge experienced experts. Every participant should leave with some new skills.

All materials are freely available on the Web at samsclass.info and will remain available after the workshop is over.

Speakers: Sam Bowne, Elizabeth Biddlecome, Kaitlyn Handelman, Irvin Lemus

SpeakerBio: Sam Bowne

Sam Bowne has been teaching computer networking and security classes at City College San Francisco since 2000. He has given talks and hands-on trainings at DEF CON, DEF CON China, Black Hat USA, HOPE, BSidesSF, BSidesLV, RSA, and many other conferences and colleges. He founded Infosec Decoded, Inc., and does corporate training and consulting for several Fortune 100 companies, on topics including Incident Response and Secure Coding.

Formal education: B.S. and Ph.D. in Physics Industry credentials:

Infosec: CISSP, Certified Ethical Hacker, Security+, Defcon Black Badge, Splunk Core Certified User Networking: Network+, Certified Fiber Optic Technician, HE IPv6 Sage, CCENT, IPv6 Forum Silver & Gold, Juniper JN0-101, Wireshark WCNA Microsoft: MCP, MCDST, MCTS: Vista

SpeakerBio: Elizabeth Biddlecome

Elizabeth Biddlecome is a consultant and instructor, delivering technical training and mentorship to students and professionals. She leverages her enthusiasm for architecture, security, and code to design and implement comprehensive information security solutions for business needs. Elizabeth enjoys wielding everything from soldering irons to cripting languages in cybersecurity competitions, hackathons, and CTFs.

SpeakerBio: Kaitlyn Handelman

Kaitlyn Handelman is an offensive security engineer at Amazon. Her focus is cybersecurity in space. In addition to traditional penetration testing, Kaitlyn works on physical devices and RF signals. In her free time, she enjoys ham radio, astronomy, and her cat, Astrocat.

SpeakerBio: Irvin Lemus, Founder at r00tkit.io

Irvin Lemus teaches people to break things so they can defend them. CISSP-certified cybersecurity professional with over a decade building competitions, teaching offensive and defensive security, and advising organizations across the Americas. Currently Director of Education & Training for Latin America at By Light and founder of r00tkit.io.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

DEF CON Workshops - (Sold Out) - Friday - 14:00-17:59 PDT

Title: Sold Out - Investigating and Responding to M365 account compromise on a shoestring: Living of the Land Incident Response

Tags: DEF CON Workshop | DEF CON Workshops

When: Friday, Aug 7, 14:00 - 17:59 PDT

Where: LVCCW Level 2 W222 (Workshops) - [Map](#)

Description:

A compromised mailbox. An inbox rule named ".". An OAuth consent to an unknown application. A sign-in from a cloud-hosting ASN with user-agent "axios" and MFA status "satisfied by claim in token". Somewhere in there is the story - and somewhere in the Microsoft 365 logs is the evidence. This four-hour hands-on workshop teaches Business Email Compromise investigation in the tenants most responders actually see: M365 Business Premium or E3. No Sentinel. No SIEM. No problem. Using only native admin centers, PowerShell modules, and a few scripts, you will run a complete BEC investigation end to end. Working through several progressive scenarios, from single-user compromise, through lateral-pivot case with MailItemsAccessed analysis, to multi-account incident with a malicious enterprise app and transport rule. You will learn how to contain, collect, triage, pivot, expand scope, remediate, and produce the three common reporting deliverables: investigation report, attestation letter, internal post-mortem. This is Living off the Land Incident Response. Through chronology and topology, come correlate some logs with me and see what story they tell.

SpeakerBio: Vince "bitpusher" Weppner

Vincent M. Weppner (Bitpusher) is an Information Security Specialist with 10+ years of dedicated cybersecurity focus and 25 years in IT overall. He works as a Security Analyst at a mid-market MSP and runs an independent IT consulting practice at theTechRelay.com. Generally found lurking in the mountains of Southern California, and occasionally maintaining his open-source tooling at github.com/bitpusher2k. His day-to-day work covers M365 security operations, Active Directory and endpoint security, BEC/ransomware incident response, EDR/SIEM management, and security consulting for SMB and mid-market clients. Specialization in Business Email Compromise was built out of direct operational need: after dozens of BEC incidents, the pattern of "which script do I need to run right now?" became clear enough to codify. Passionately solving puzzles through scripting, and hoping to pass on some of it to you.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

DEF CON Workshops - (Sold Out) - Friday - 09:00-12:59 PDT

Title: Sold Out - Learning to Hack Bluetooth Low Energy with BLE CTF

Tags: DEF CON Workshop | DEF CON Workshops

When: Friday, Aug 7, 09:00 - 12:59 PDT

Where: LVCCW Level 2 W232 (Workshops) - [Map](#)

Description:

BLE CTF is a series of Bluetooth Low Energy challenges in a capture-the-flag format, created to teach the fundamentals of interacting with and hacking BLE services. Each flag interactively introduces a new concept.

Over the years, BLE CTF has expanded across platforms and skill levels. Books, workshops, trainings, and conferences have adopted it as both an educational platform and CTF. As an open source, low-cost, extensible solution, it has helped advance Bluetooth security research.

This workshop teaches the fundamentals of hacking BLE through hands-on exercises that introduce beginners to new concepts while giving experienced users a chance to try new tools and techniques. After completing it, you will have a solid understanding of how to hack BLE devices in the wild.

New for DEF CON 34: the workshop uses a brand new variant of BLE CTF built specifically for this event. Returning students will face fresh challenges they have not seen before, and the new exercises are designed to resist online walkthroughs and LLM-assisted shortcuts. We will also introduce new client tools, including gratttool, a modern replacement for gatttool (which has been deprecated from most Linux distributions). Whether this is your first BLE CTF or your eighth, you will leave with new skills and tools.

Speakers: Ryan "Hackgnar" Holeman, Alek Amrani

SpeakerBio: Ryan "Hackgnar" Holeman

Ryan Holeman resides in Austin, Texas, where he works as the CISO for Stability AI. He holds a Ph.D. in cyber defense from Dakota State University and has spoken at respected venues such as Black Hat, DEF CON, Lockdown, BSides, Ruxcon, Notacon, and Shmoocon. You can keep up with his current activity, open source contributions, and general news on his blog. His spare time is mostly spent digging into various network protocols, random hacking, creating art, surfing, and shredding local skateparks.

SpeakerBio: Alek Amrani

Alek Amrani runs the security team at Cape.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Sold Out - Learning to Reverse Engineer Compiled C as We Learn to Write It

Tags: DEF CON Workshop | DEF CON Workshops

When: Saturday, Aug 8, 14:00 - 17:59 PDT

Where: LVCCW Level 2 W232 (Workshops) - [Map](#)

Description:

Software reverse engineering is a fundamental skill: a prerequisite to engaging with many fields of study in computer security that depend on low-level knowledge. Malware analysis, vulnerability research, offensive tool development, and digital forensics all involve the analysis of code which has been compiled, obfuscated, or otherwise stripped of useful names, data types, comments, and other human-readable information. Without the ability to read disassembled code, you will not be able to understand code that your computer will happily execute.

In this workshop, I will guide you through learning to read disassembled code *while* you learn C. We will progress through the C programming language's constructs with as few assumptions as possible about your background, and at each stage we will reverse engineer the compiler's output in Ghidra and trace through with a debugger to understand the generated code. You do not need any prior experience in programming.

I will also be demonstrating useful techniques for using locally-hosted large language models to aid in the learning process. Use AI to improve your own skillset, rather than using it to do the work for you.

SpeakerBio: Wesley McGrew, Senior Cyber Fellow at MartinFed

Dr. Wesley McGrew directs research, development, reverse engineering, and offensive cyber operations as Senior Cybersecurity Fellow for MartinFederal. He has presented at DEF CON and Black Hat USA on topics of penetration testing, malware analysis, critical infrastructure, and vintage computing, and has taught self-designed courses on reverse engineering and cyber operations at Mississippi State University. Wesley has a Ph.D. in Computer Science from Mississippi State University for his research in vulnerability analysis of SCADA HMI systems. He has entertained audiences at many DEF CON parties as a house music DJ, as well.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

DEF CON Workshops - (Sold Out) - Friday - 09:00-12:59 PDT

Title: Sold Out - Long Live Empire: A C2 Workshop for Modern Red Teaming

Tags: DEF CON Workshop | DEF CON Workshops

When: Friday, Aug 7, 09:00 - 12:59 PDT

Where: LVCCW Level 2 W231 (Workshops) - [Map](#)

Description:

Behind every breach report from the last decade is a Command and Control (C2) framework. C2 is how operators reach into a compromised network, move sideways, harvest credentials, and stay invisible. This 4-hour, hands-on workshop puts you in the operator's chair. You set up your own Empire team server, learn the listener-stager-agent model from scratch, and run seven exercises that take you from "never touched a C2" to dumping credentials off a box you compromised yourself.

You'll spin up an HTTP listener, deploy a .NET agent to a Windows target, and run post-exploitation tradecraft: Rubeus for credentials, SharpHound for AD enumeration, port-forward pivots to internal hosts, and privesc modules that turn a foothold into full control. You'll even build a custom Empire plugin that auto-runs on every new agent. The capstone is a mini-CTF on a cloud-hosted range we keep open all weekend, with a prize for the winners.

You leave with the mental model most operators take years to build: how modern C2 actually works, what it assumes about the target, and where defenders most often catch it. No VMs to download. No setup before class. Bring a laptop, get on WiFi, and we'll have agents running before the first break.

Speakers: Jake "Hubbl3" Krasnov, Vincent "Vinnybod" Rose, Anthony "Coin" Rose, Dan Niefeld

SpeakerBio: Jake "Hubbl3" Krasnov

Jake "Hubble" Krasnov is the Red Team Operations Lead at BC Security, with a distinguished career spanning engineering and cybersecurity. A U.S. Air Force veteran, Jake began his career as an Astronautical Engineer overseeing rocket modifications, leading test and evaluation efforts for the F-22, and conducting red team operations with the 57th Information Aggressors. He later served as a Technical Lead Engineer at Boeing Phantom Works, where he focused on embedded security for aviation and space defense projects. A seasoned speaker and trainer, Jake has presented at DEF CON, Black Hat, HackRedCon, HackSpaceCon, and HackMiami, and has previously taught Empire and offensive PowerShell at DEF CON.

SpeakerBio: Vincent "Vinnybod" Rose

Vincent "Vinnybod" Rose is the Lead Developer for Empire and Starkiller. He is a software engineer with a decade of expertise in building highly scalable cloud services, improving developer operations, and automation. Recently, his focus has been on the reliability and stability of the Empire C2 server. Vinnybod has presented at Black Hat and has taught courses at DEF CON on Red Teaming and Offensive PowerShell. He currently maintains a cybersecurity blog focused on offensive security at <https://bcsecurity.io/blog/>.

SpeakerBio: Anthony "Coin" Rose

Dr. Anthony "Coin" Rose is an officer in the United States Air Force, an Assistant Professor, and the Director of the Center for Cyberspace Research at the Air Force Institute of Technology. He holds a doctorate in Electrical Engineering and has expertise in machine learning, with a focus on its application to cybersecurity and malware detection. He is also the founder of SIMAPTIC and the Director of Security Research at BC Security, where he specializes in adversary tactics and emulation planning, Red and Blue Team operations, and embedded systems security. Dr. Rose is credited with 16 CVEs and has presented at numerous security conferences, including Black Hat, DEF CON, HackSpaceCon, HackMiami, and RSA Conference.

SpeakerBio: Dan Niefeld

Dan Niefeld is the founder of several Cyber Security and Technology organizations. An accomplished social engineer his career has spanned from program management to organizing conferences like Hack Space Con, Dan has spent his career, educating, mentoring and developing disrupting technologies with a focus of Mission and Community Development.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

DEF CON Workshops - (Sold Out) - Friday - 09:00-12:59 PDT

Title: Sold Out - Malware Development 101 - From Zero to Hero: Adapt your payload to your environment

Tags: DEF CON Workshop | DEF CON Workshops

When: Friday, Aug 7, 09:00 - 12:59 PDT

Where: LVCCW Level 2 W230 (Workshops) - [Map](#)

Description:

This workshop will give an initiation to offensive malware development in C/C++ and how it is possible to adapt the approach depending on the security solution that must be tackled down. Different methods such as ModuleStomping, DLL Injection, Threadless Injection and Hardware Breakpoint for dehooking will be seen. The idea is to start with a basic malware performing process injection and apply additional techniques to start evading EDR. At each step, some analysis on the malware will be performed to understand the differences at the system level and the IOC detected by the EDR. At the end of this workshop, you will have all the knowledge needed to develop your own malware and adapt it to the targeted environment to escape from the basic pattern and spawn your beacons as if EDR didn't exist.

SpeakerBio: Yoann "OtterHacker" DEQUEKER

Yoann Dequeker (@OtterHacker) is a red team operator at Wavestone entitle with OSCP and CRT0 certification. Aside from his RedTeam engagements and his contributions to public projects such as Impacket, he spends time working on Malware Developpement to ease beacon deployment and EDR bypass during engagements and is currently developing a fully custom C2.

His research leads him to present his results on several conferences such as LeHack (Paris), Insomni'hack (Swiss) or even through a 4-hour malware workshop at Defcon31,32 and 33 (Las Vegas). All along the year, he publishes several white papers on the techniques he discovered or upgraded and the vulnerabilities he found on public products.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

DEF CON Workshops - (Sold Out) - Friday - 09:00-12:59 PDT

Title: Sold Out - Offensive Packet Wizardry with Scapy

Tags: DEF CON Workshop | DEF CON Workshops

When: Friday, Aug 7, 09:00 - 12:59 PDT

Where: LVCCW Level 2 W222 (Workshops) - [Map](#)

Description:

Offensive Packet Wizardry with Scapy is a four-hour, 100% hands-on workshop that teaches attendees to build offensive networking tools from scratch in Python using Scapy, the packet crafting library used by red teams, malware analysts, and vulnerability researchers worldwide.

Starting from first principles, raw packet construction, layer stacking, and send/receive mechanics, the workshop moves progressively through active reconnaissance, ARP cache poisoning with live credential interception, TCP/IP stack abuse (session injection, SYN flood, RST killing), protocol fuzzing against an intentionally vulnerable binary service, and full covert channel implementation (ICMP C2 shell, DNS file exfiltration, TCP header steganography).

Every technique is implemented live in Python against an isolated lab network. Students leave with a working, importable red team toolkit, a Python package with a unified CLI, that they built themselves and can adapt for future engagements.

The workshop concludes with "Silent Pivot", a scored capstone scenario that chains all techniques into a realistic kill chain: stealth discovery, service identification, fuzzer- triggered crash, ICMP command execution, DNS exfiltration of /etc/shadow, and network cleanup, all subject to an IDS alert budget.

SpeakerBio: Mike "Chicolinux" Guirao

Mike "Chicolinux" Guirao began his journey in the security field roughly 25 years ago while completing a master's degree. Since then, they have developed both broad and deep expertise across this incredible discipline. Currently, they are pursuing a PhD at New Mexico State University, where their research intersects Cybersecurity and Machine Learning/Artificial Intelligence.

In addition to their academic pursuits, Mike serves on the organizing team for the Crypto & Privacy Village. This marks their third time teaching a workshop at DEF CON since DEF CON 24. They also hold several notable industry certifications, including the SANS GCIH, ISC2 CC, and Linux+, and they are excited to share their wealth of experience and knowledge.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

DEF CON Workshops - (Sold Out) - Friday - 14:00-17:59 PDT

Title: Sold Out - OT Systems: how to secure them in practice!

Tags: DEF CON Workshop | DEF CON Workshops

When: Friday, Aug 7, 14:00 - 17:59 PDT

Where: LVCCW Level 2 W225 (Workshops) - [Map](#)

Description:

Securing OT systems is often presented as challenging, with multiple business constraints - but is it that complicated, especially considering a single industrial site? In this 4-hour, hands-on workshop, each participant will manipulate a simple but realistic Industrial Control System setup with SCADA systems & PLCs. Attendees will have the opportunity to secure it step by step, through several hands-on exercises & discover how to manually secure OT systems: OT inventory, backups, network security, system hardening and detection. What if the real challenge is OT security at scale? Besides implementing manual security on our setup, we will address each step of the way OT security at scale and share feedback on how large companies are securing their OT systems, both at organizational & technical level: community of OT cyber correspondents, OT DMZ and security tools deployment. No prior OT experience is required.

Speakers: Alexandrine Torrents, Arnaud SOULLIE

SpeakerBio: Alexandrine Torrents

Alexandrine Torrents is a cybersecurity expert at Wavestone. She started as a penetration tester, and then specialized in OT cybersecurity. She is IEC 62443 certified. She performed dozens of OT cybersecurity assessments across various industries & worked on OT models to perform attacks on PLCs & SCADA systems. Alexandrine also helps secure OT both at technical & organization levels: secure architecture, system hardening, IAM, cyber resilience, detection, governance, awareness & training, risk assessment, cyber by design, etc. Alexandrine works with different CISOs on their OT cybersecurity roadmaps & programs at different scales of large industrial companies: site, business units, Group with worldwide scope. Alexandrine also gives training on OT cybersecurity.

SpeakerBio: Arnaud SOULLIE

Arnaud Soullie is a Senior Manager at Wavestone. He has over 15 years of experience in security assessments and penetration testing, with 10 years specializing in Industrial Control Systems cybersecurity. He has delivered talks and workshops at DEF CON, Black Hat Europe, BruCON, CS3STHLM, BSides Las Vegas, and others. He is the creator of the DYODE open-source data diode project and has been teaching ICS cybersecurity since 2015.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

DEF CON Workshops - (Sold Out) - Sunday - 09:00-12:59 PDT

Title: Sold Out - Pivot, Hunt, Publish: An Offline, Hands-On CTI Workshop for Blue Teams and Threat Researchers

Tags: DEF CON Workshop | DEF CON Workshops

When: Sunday, Aug 9, 09:00 - 12:59 PDT

Where: LVCCW Level 2 W233 (Workshops) - [Map](#)

Description:

Cyber Threat Intelligence is the most overspecified and underspecified discipline in security. Every vendor sells a feed. Every conference has a track. Every blog post claims attribution. And yet - most blue teams still drown in IOCs they cannot operationalize, and most aspiring threat researchers do not know how to pivot from a single sample to a discovered campaign.

This workshop fixes both problems in four hours, fully offline, with every minute of those four hours spent on content rather than setup, and without distributing a single piece of malware.

SpeakerBio: Rushikesh Nandedkar

Rushikesh is a researcher. Having more than 10 years of experience under his belt, his assignments have always been pointed towards reducing the state of insecurity for information. His research papers were accepted at the nullcon '14 '18 '20 '21, BruCON '16 '17 '18 '19 '21, Blackhat USA Arsenal '18 '19 '25, DEFCON 24 26 27, x33fcon '17 '18 '20 '21, BSides Delhi '17 '20, c0c0n '17 '25, HITCON '14, NCACNS '13 + co-author of "DARWIN" (use cases for covert wireless), "DECEPTICON", an intelligent evil-twin and "SASTRI", Plug and Play VM for SAST and author of ARC (Artefact Reuse Comparator) and Q-TIP (QR Code Threat Inspection Platform). Being an avid CTF player, for him, solace is messing up with packets, frames, and shellcodes while attempting to reach the state of void *.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

DEF CON Workshops - (Sold Out) - Sunday - 09:00-12:59 PDT

Title: Sold Out - Post-Quantum Cryptography (PQC) for Hackers

Tags: DEF CON Workshop | DEF CON Workshops

When: Sunday, Aug 9, 09:00 - 12:59 PDT

Where: LVCCW Level 2 W228 (Workshops) - [Map](#)

Description:

Secure communications are not a luxury ,Ät they are a foundational requirement for human dignity in the digital age. Our most meaningful conversations, transactions, and decisions demand end-to-end encryption, strong authentication, and verifiable integrity. The notion that "only those with something to hide need strong crypto" is not merely lazy; it is dangerously shortsighted. Privacy is the space where autonomy, intimacy, and authentic human experience thrive. When that space is violated, the damage ripples far beyond the individual.

For decades, classical public-key cryptography has quietly protected everything from online banking to private messaging. That era is ending. Quantum computers are advancing rapidly, and the break of today's asymmetric algorithms ,Ät often called the Quantum Apocalypse ,Ät is no longer a question of if, but when. The window to prepare is narrowing. Migration must begin now.

In this workshop, you'll implement PQC algorithms from the NSA's CNSA Suite 2.0. You'll use C++, OpenSSL and Linux to demonstrate the secure usage of ML-KEM, ML-DSA, AES-256, and SHA-512. You'll leave with clean, reusable code, deep implementation insight, and the practical skills needed to integrate PQC into real-world systems.

We might not all have something to hide, but we all have something worth protecting.

SpeakerBio: Eric "Eijah" Anderson

Eijah is the founder of Code Siren, LLC and has 25+ years of experience in software development. He is the creator of Polynom, the world's first CNSA Suite 2.0 PQC collaboration app and the author of multiple FIPS 140-3 modules. He is also the developer of Demonsaw, an encrypted communications platform that allows you to share information without fear of data collection or surveillance. Before that Eijah was a Lead Programmer at Rockstar Games where he created Grand Theft Auto V and Red Dead Redemption 2. In 2007, Eijah hacked multiple implementations of the Advanced Access Content System (AACS) protocol and released the first Blu-ray device keys under the pseudonym, ATARI Vampire. He has been a faculty member at multiple colleges, has spoken at DEF CON and other security conferences, and holds a master's degree in Computer Science. Eijah is an active member of the hacking community and is an avid proponent of Internet freedom.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

DEF CON Workshops - (Sold Out) - Sunday - 09:00-12:59 PDT

Title: Sold Out - Purple Protocol: Adversary emulation for everyone

Tags: DEF CON Workshop | DEF CON Workshops

When: Sunday, Aug 9, 09:00 - 12:59 PDT

Where: LVCCW Level 2 W229 (Workshops) - [Map](#)

Description:

Have you ever been curious about the techniques used by most notorious hackers to infiltrate some of the world's biggest networks? What would happen if they attacked yours? Companies burn millions of dollars in cybersecurity defenses, yet breaches still happen. Why? Because victory favors the prepared, not the well-funded.

This beginner friendly workshop explores a practical way to test your defenses. You will learn to organize and execute a Threat Intelligence-led Purple Team Engagement with Open Source tooling. You will learn how to select relevant Threat Actors, execute test cases, document results, generate action items for the Blue Team to remediate, and report the results in a way that even executives can understand. (Spoiler: They like Pie Charts, Line Graphs, and bright colors) This will all be done on a VM we will provide with the Open Source tooling pre-installed. Everything learned in this course can be replicated at your organization.

Join us in this workshop to learn why Purple Teaming is undeniably one of the most methodical and effective ways to improve your resilience against the threat actors most likely to attack your organization.

Speakers: Patrick "PilotPat" Raiden, Ben "Marba\$" Strout, Brandon "D43m0n" Kraycirik

SpeakerBio: Patrick "PilotPat" Raiden

Patrick has been working in Cybersecurity for the past decade, ranging from Security Engineering, Vulnerability Management, Penetration Testing, and Red Team Ops. ↯ He holds industry certs including the OSCP, CRT0 and GRTP. ↯ He led the effort to build a new Purple Team program at one of the largest healthcare organizations in the United States and continues to manage the program. Patrick is also a DEF CON Black Badge winner.

SpeakerBio: Ben "Marba\$" Strout

Marba\$ leads an Offensive Security Team and research vulnerabilities at one of the largest U.S. healthcare conglomerates. With experience spanning healthcare, biotech, pharma, and fintech, his work centers on application security, red teaming, and automation. He is the founder of DC207- Maine's DEF CON group - and the General Chair / Lead Organizer of BSides Maine.

SpeakerBio: Brandon "D43m0n" Kraycirik

D43m0n is a senior cyber security research engineer for one of the largest banking institutions in the world. Having over five years of experience in offensive security, specializing in red teaming, vulnerability research, and custom tool development.

He holds advanced certifications that include OSCE3, BSCP, CRT0, CARTP, and eWPTX. While doing so, he was contributing to the cyber security community as the discoverer of CVE-2025-26332 (Dell) and CVE-2025-30398 (Microsoft), while also having authored *„ÄúDebugging CVE-2023-37679: A Step-by-Step Guide to Fixing the Windows Exploit.„Äù*

One of his most recent accomplishments at DEF CON is finally obtaining the accolade of being a Black Badge holder.

Outside of cybersecurity, he is a passionate researcher with a deep appreciation for the outdoors.



DEF CON Workshops - (Sold Out) - Saturday - 14:00-17:59 PDT

Title: Sold Out - Purple Teaming Industrial Control Systems

Tags: DEF CON Workshop | DEF CON Workshops

When: Saturday, Aug 8, 14:00 - 17:59 PDT

Where: LVCCW Level 2 W225 (Workshops) - [Map](#)

Description:

Security monitoring is often presented as the silver bullet for Industrial Control System (ICS) security ,Ä but how effective is it against realistic adversaries? In this 4-hour, hands-on workshop, participants will use CALDERA, the open-source adversary emulation framework, to conduct purple-team exercises against simulated & live industrial environments. Attendees will simulate real-world IT and OT attacks, observe what is (and is not) detected across EDR, logs, and network monitoring, and map results to MITRE ATT&CK for ICS. Rather than focusing on exploitation alone, this workshop teaches a repeatable methodology to assess detection coverage, identify OT blind spots, and improve monitoring strategies. Participants leave with concrete techniques they can apply in their own environments ,Ä from tabletop exercises to continuous detection testing.

Speakers:Arnaud SOULLIE,Alexandrine Torrents

SpeakerBio: Arnaud SOULLIE

Arnaud Soullie is a Senior Manager at Wavestone. He has over 15 years of experience in security assessments and penetration testing, with 10 years specializing in Industrial Control Systems cybersecurity. He has delivered talks and workshops at DEF CON, Black Hat Europe, BruCON, CS3STHLM, BSides Las Vegas, and others. He is the creator of the DYODE open-source data diode project and has been teaching ICS cybersecurity since 2015.

SpeakerBio: Alexandrine Torrents

Alexandrine Torrents is a cybersecurity expert at Wavestone. She started as a penetration tester, and then specialized in OT cybersecurity. She is IEC 62443 certified. She performed dozens of OT cybersecurity assessments across various industries & worked on OT models to perform attacks on PLCs & SCADA systems. Alexandrine also helps secure OT both at technical & organization levels: secure architecture, system hardening, IAM, cyber resilience, detection, governance, awareness & training, risk assessment, cyber by design, etc. Alexandrine works with different CISOs on their OT cybersecurity roadmaps & programs at different scales of large industrial companies: site, business units, Group with worldwide scope. Alexandrine also gives training on OT cybersecurity.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

DEF CON Workshops - (Sold Out) - Friday - 14:00-17:59 PDT

Title: Sold Out - Reaching Mythos: Hands-On Vulnerability Discovery with Local AI Models

Tags: DEF CON Workshop | DEF CON Workshops

When: Friday, Aug 7, 14:00 - 17:59 PDT

Where: LVCCW Level 2 W229 (Workshops) - [Map](#)

Description:

Anthropic, April 2026: Claude Mythos Preview is "strikingly capable" at zero-day discovery. They chose not to release it.

AISLE, one week later: "The moat in AI cybersecurity is the system, not the model." They reproduced Mythos-class findings on FreeBSD with a 1,700-line scan.py and a commodity model for under \$100.

This four-hour hands-on workshop is the local-hardware version of that argument. Two reproductions, two domains, one harness pattern.

Part I: point AISLE's open-source pipeline at a pre-patch FreeBSD checkout through a hosted local-AI inference endpoint and reproduce the 17-year-old CVE-2026-4747 that drove Mythos, for sub-dollar spend.

Part II: change domains. Drive Ghidra through MCP tool calls against unpatchable D-Link DNS-320L firmware. Validate CVE-2024-3273 with the advisory in hand, then rediscover it from a blank start once the harness moves enumeration into the driver.

What happens next is what you come to find out. Same hardware, same model, same harness, four hours later: can local AI extend the famous disclosure with bugs the original missed? Come see for yourself.

No GPU. No API. No cloud spend. The workshop hosts inference for the room.

SpeakerBio: John "clearbluejar" McIntosh

John McIntosh (@clearbluejar) is a security researcher and founder of ClearSecLabs, specializing in reverse engineering, vulnerability research, and AI-assisted binary analysis. He is the author of ghidriff, an open-source Ghidra-based binary diffing engine, and pyghidra-mcp, a headless Ghidra MCP server enabling LLM-driven, project-wide, multi-binary reverse engineering workflows. An active contributor to the Agent Skills ecosystem, John bridges deterministic analysis with AI-driven reasoning to accelerate vulnerability research. He has delivered training and workshops at DEF CON, Black Hat, REcon, Ringzer0, 44CON, Objective by the Sea, and Insomni'hack, covering topics from practical Windows reverse engineering to building private local LLM RE stacks. His recent work includes the "Agentic RE" training at DEF CON Singapore 2026, the MCP Ghidra workshop at REcon 2025, and the "Supercharging Ghidra" LLM workshop at Ringzer0 COUNTERMEASURE 2025. With over a decade of offensive security experience, John publishes detailed research on reversing CVEs, building RE tooling, and agentic patch diffing at clearbluejar.github.io. His teaching emphasizes reproducibility, progressive skill-building, and contributor empowerment.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Sold Out - Salesforce Apex Predator: Breaking Salesforce Sites

Tags: DEF CON Workshop | DEF CON Workshops

When: Saturday, Aug 8, 14:00 - 17:59 PDT

Where: LVCCW Level 2 W233 (Workshops) - [Map](#)

Description:

Salesforce Sites are one of the most under-tested attack surfaces in enterprise security. When pentesters encounter them, most skip past - the Aura framework doesn't behave like a standard web application, and standard web testing techniques don't apply. Salesforce sites run on proprietary frameworks (Aura and LWR) with their own API surfaces, access models, and injection patterns. In March 2026, ShinyHunters demonstrated what that blind spot costs: sensitive data exfiltrated from hundreds of organizations through sites no one had tested.

This workshop teaches pentesters and red teamers a complete offensive methodology for Salesforce Experience Sites, going well past the record enumeration that makes up most public guidance on the topic.

Attendees will enumerate objects and dump records via the Aura API, then learn to identify and invoke custom Apex controllers running in system mode - controllers that bypass standard access management mechanisms, and which are surprisingly common and criminally underexplored. We cover SOQL injection in depth: why normal SQL injection tests fail, and how to exploit it. We cover deterministic route enumeration as an unauthenticated user, and LWR sites - Salesforce's next-generation framework - including the release of LWRed, a new open-source scanner built specifically for them.

Speakers: Nitay Bachrach, Cynthia Ardman

SpeakerBio: Nitay Bachrach

Nitay Bachrach is a security researcher at Reco (Tel Aviv, Israel) specializing in offensive security research against enterprise SaaS platforms. He is a pioneer in Salesforce offensive security: he published new exploitation methods for the Aura framework, discovered the Einstein Wormhole vulnerability and a Public Link exploitation technique in Salesforce's platform, and identified and responsibly disclosed critical vulnerabilities in dozens of major Salesforce deployments. His research extends to Okta, GCP, and other enterprise platforms. He spoke at Insomni'hack on "Neo4jection" - novel graph injection techniques against Neo4j. In May 2026, he is running a Salesforce-focused CTF event in Tel Aviv. The LWR exploitation methodology and LWRed tool premiering at this workshop represent previously unpublished research from original work on Salesforce's next-generation Experience Site framework.

SpeakerBio: Cynthia Ardman

Cynthia has spent 10+ years making life harder for attackers. She currently builds threat detection at Reco, and previously did the same at AppOmni, AWS, and Snowflake, places where "the blast radius" isn't a metaphor. At AWS she developed MITRE ATT&CK-mapped detection for corporate infrastructure, partnered with the Red Team to close gaps they found, and led a project that knocked hacking tool presence down by 30%. At Snowflake she ran blue team ops and built the SQL-based alerting pipeline from scratch. At StubHub she hunted down an active intrusion by tracing logs across systems and performed the root cause analysis so it wouldn't happen twice. She came up through desktop support, building Linux blade servers and remediating malware on customer machines, the kind of work that teaches you what actually breaks. CISSP. Splunk ES Admin. Writes Python when she has to and JSONata when nobody's looking.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

DEF CON Workshops - (Sold Out) - Friday - 14:00-17:59 PDT

Title: Sold Out - Solder, Detect, Listen: Build Your Own EMF Explorer

Tags: DEF CON Workshop | DEF CON Workshops

When: Friday, Aug 7, 14:00 - 17:59 PDT

Where: LVCCW Level 2 W230 (Workshops) - [Map](#)

Description:

Every electronic device around you is silently broadcasting electromagnetic signals. In this hands-on workshop, you will build an SMD (surface-mount) version of the EMF Explorer from bare PCB to working device, learning progressive SMD soldering techniques from 1206 down to 0603 component sizes along the way. Geared for absolute beginners who are new to soldering and electronics. This session pairs each build stage with a circuit theory deep dive: you will understand the voltage divider powering your board, the op-amp gain stages amplifying EMF signals into audible sound, and how inductor geometry shapes what you can hear. Walk away with a functional EMF listening device, new SMD skills transferable to real-world hardware hacking, and a deeper understanding of the electromagnetic emissions all around you.

SpeakerBio: Darcy "@Drc3p0" Neal

Darcy Neal (Drc3p0) is an electronics educator and founder of SporkLogic, where they design open-source hardware kits and facilitate soldering workshops at maker and hacker events worldwide. With over 15 years in interactive audio-visual hardware design, Darcy's work spans RF experimentation, new media installations, boutique synthesizer production, and hands-on electronics education. Their flagship product, the EMF Explorer, is an accessible tool for sonifying electromagnetic fields. They collaborate regularly with Mitch Altman and the Hardware Hacking Assembly, and have taught large-scale soldering workshops across the global hacker community.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Sold Out - Step-by-Step Malware Development: Evading EDR from Loaders to the Kernel

Tags: DEF CON Workshop | DEF CON Workshops

When: Saturday, Aug 8, 09:00 - 12:59 PDT

Where: LVCCW Level 2 W228 (Workshops) - [Map](#)

Description:

Endpoint Detection and Response (EDR) systems are key parts of modern security. This workshop provides a guide for custom malware development, C2 customization, defense evasion, and kernel exploitation. We will use Elastic Defend throughout the session. By analyzing detection logs and rules, we will understand what EDR monitors and why payloads are caught step by step.

After a short overview of Windows defenses and EDR, we focus on malware development. Participants will implement typical malware techniques, such as APC Injection, Thread Hijacking, Fiber and Module Stomping in multiple languages. Next, we learn about call stack analysis. Attendees will implement Stack Spoofing and Indirect Syscalls to hide execution flows and bypass stack analysis.

The workshop then moves to C2 customization using the Havoc C&C framework. By combining custom loaders with C2 source code modifications, participants will bypass static signatures, behavioral rules, and AI detection to successfully establish a C2 session.

Finally, we'll demonstrate the possibilities of Bring Your Own Vulnerable Driver (BYOVD) attacks for the post-exploitation phase. When we have access to the kernel space, we can take more aggressive measures. We'll use some vulnerable drivers to kill or blind an EDR sensor itself.

Speakers: Yu Terada, Kotaro "@Decamark / @BinaryPoodle" Osugi

SpeakerBio: Yu Terada

Yu Terada is a security researcher and a red team consultant for Fujitsu. He worked as a SOC Analyst and CSIRT for over five years. In 2021, he joined the company as a Security Researcher. He is primarily involved in developing new attack methods and tools. He also participates in internal red team activities and cyber exercises. He has spoken at Black Hat USA/Europe, BSides Las Vegas, Code Blue, and several conferences in Japan. He holds a Master's degree in Computer Science, as well as certifications including OSEP, OSCP, CRTL, CETP, ODPC, CISSP, GIAC, etc.

SpeakerBio: Kotaro "@Decamark / @BinaryPoodle" Osugi

Kotaro Osugi is a security researcher and a red team consultant who has his profession in reverse-engineering. His research area includes malware analysis and binary exploitation. He has given a speech at BHEU Arsenal about a tool for kernel exploitation. OSED and OSEE certified.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

DEF CON Workshops - (Sold Out) - Friday - 09:00-12:59 PDT

Title: Sold Out - Web Hacking 101

Tags: DEF CON Workshop | DEF CON Workshops

When: Friday, Aug 7, 09:00 - 12:59 PDT

Where: LVCCW Level 2 W229 (Workshops) - [Map](#)

Description:

Most security training starts with slides. This workshop starts with a target. Students spend the majority of the course attacking a purpose-built web application across progressive labs covering the vulnerability classes that define modern web security.

Each module follows a difficulty curve. Entry-level labs present classic, unfiltered vulnerabilities for students to exploit independently. Difficulty escalates as filters and defenses appear, requiring adaptation and creative problem-solving. Failed payloads, broken assumptions, and dead ends are not setbacks. They are the learning journey. The frustration of a blocked payload and the persistence to find the bypass is how offensive intuition is built.

A final exploit chaining challenge ties everything together, combining findings across vulnerability classes to demonstrate how moderate issues chain into critical impact, the way real attacks work.

Students attack, fail, adapt, and break through. Hands-on exploitation and the willingness to struggle is the foundation of any security career. It starts here.

All you need is a laptop and persistence.

Speakers:cale "calebot" smith,Ruchik Dave,Young Seuk Kim,Luke Cycon

SpeakerBio: cale "calebot" smith

Cale Smith has spent his entire life obsessed with one question: "Yeah, but how does it actually work?"

He started out building things, then realized breaking them was more fun, and has been doing exactly that across web, cloud, binary, IoT, and mobile ever since. He now manages a device-focused security team at Amazon, where his "what if I just..." instincts are finally considered a job qualification.

SpeakerBio: Ruchik Dave

Ruchik Samir Dave is a software engineer and security specialist with nearly 20 years of experience at the intersection of complex systems security and emerging threat landscapes. Ruchik has contributed to security frameworks for aviation systems and privacy-compliant architectures for large consumer IoT ecosystems, bringing safety-critical systems expertise to emerging technology platforms. His current research explores cloud security paradigms, security compliance, AI-assisted threat detection systems, and the novel attack surfaces introduced by machine learning implementations in embedded environments, areas that represent the cutting edge of adversarial research and defensive innovation. With a passion for building secure, large-scale software systems, Ruchik's work addresses the evolving security challenges where traditional cybersecurity meets artificial intelligence, IoT proliferation, and safety-critical infrastructure.

SpeakerBio: Young Seuk Kim

Husband, father, hacker, gamer. Young's path into security started like a good game exploit, he wanted to win, bent the rules, and discovered a passion for hacking. He began as a web app security consultant, moved into penetration testing and red teaming, and now works in application security engineering, helping teams build secure systems (and still breaking things for fun). He also dives into all kinds of games and stories, especially fantasy with Eastern martial arts, and loves dissecting media with the same curiosity he brings to code.

SpeakerBio: Luke Cycon

Luke is a former builder turned security engineer at Amazon, focused on web, cloud, and embedded device security. He came up building things before he discovered that breaking them taught him more about how they really work. These days he likes to poke at things until they misbehave, then help the builders make sure it doesn't happen twice. Off the clock, you'll find him tinkering with hardware, firing lasers at something, and celebrating each fixed bug with a bit too much whisky.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

DEF CON Workshops - (Sold Out) - Saturday - 09:00-12:59 PDT

Title: Sold Out - Wi-Fight Club: I am Jack's Evil Twin

Tags: DEF CON Workshop | DEF CON Workshops

When: Saturday, Aug 8, 09:00 - 12:59 PDT

Where: LVCCW Level 2 W222 (Workshops) - [Map](#)

Description:

'Wi-Fight Club: I am Jack's Evil Twin' will teach you how to deploy rogue AP (Evil Twins) in your client's environment. Using rogue APs lets you test your client's Wireless Intrusion Detection System, passwords, wireless phishing education, and overall wireless security.

We will discuss rogue AP Tactics, Techniques, and Procedures, and how / why they work. In this workshop you will set up a CAPTIVE PORTAL, WPA2, and 802.1x rogue AP. We will also go over OWE and WPA3-SAE transition mode attacks.

We will walk through a scenario at a client's site, then set up a rogue AP to harvest user credentials for the various client networks. We will then crack the harvested credentials. We will finish up with a section on defense. We will be using EAPHAMMER, HOSTAPD-MANA, WIFIPHISHER, and AIRBASE-NG for the rogue AP section. HASHCAT, Aircrack-ng, and John for the password cracking section. This workshop is for beginners, but participants should have basic Linux and 802.11 knowledge and be comfortable using virtual machines.

Speakers: James Hawk, Jon "C4V3M4N" Milkins, Brian Burnett

SpeakerBio: James Hawk

James Hawk (He/Him) is a Principal Consultant with Google Public Sector within Proactive Services. He is the wireless subject matter expert for his team. James has led and contributed to numerous assessments (Red Teams and pentests). He has developed internal training and tool updates for 802.11 for his company. James is a 20-year veteran of the U.S. Army and has over 10 years of hands-on experience in wireless technologies. James is constantly researching/testing 802.11 attacks against his home lab. He is a fan of hockey, LetterKenny, and almost anything sci-fi.

SpeakerBio: Jon "C4V3M4N" Milkins

Jon Milkins (He/Him) is a principal penetration tester focusing on all types of penetration tests from network-based to web applications and APIs to more recently wireless networks. He has developed training and pentest utilities throughout his career to help advance team capabilities. He is a former Army veteran and is attempting to curate small and efficient rulesets for Hashcat in his free time to aid in wireless hash cracking. In his free time, he enjoys playing and running TTRPGs like Delta Green, password cracking, and making hard cider.

SpeakerBio: Brian Burnett

Brian Burnett is the founder of Offensive Technical Solutions (OTS) where he conducts web-application, internal network, and cloud penetration tests. Prior to founding OTS, he served five years in the United States Army, followed by seven years supporting internal teams at Fortune 500 companies. Brian holds degrees in computer science, pentesting, theology, and Russian. He enjoys tinkering with his home lab, collecting certifications, and committing poorly written code. His hobbies include Brazilian Jiu-Jitsu, purchasing unnecessary power tools, and CrossFit.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

DEF CON Workshops - (Sold Out) - Saturday - 09:00-12:59 PDT

Title: Sold Out - Words As Weapons: Breaking AI and Agents; Then Securing Them

Tags: DEF CON Workshop | DEF CON Workshops

When: Saturday, Aug 8, 09:00 - 12:59 PDT

Where: LVCCW Level 2 W229 (Workshops) - [Map](#)

Description:

Most "AI security" talks stop at the slide that says "prompt injection is bad." This workshop does the opposite. Attendees spend four hours inside a working, vulnerable production-style AI system - a mock car dealership backed by a real LLM, a real database, and real tool calls - and learn to break it, watch it break, then put it back together with defenses that actually hold. You will: (1) manipulate prices and inventory using direct and indirect prompt injection, (2) reproduce an EchoLeak-style zero-click data exfiltration against a RAG pipeline, (3) execute a model-extraction attack against a deployed classifier, and Each of these modules will layer in defenses one at a time to see how the AI reacts. We close by mapping everything to OWASP LLM Top 10, OWASP Agentic Top 10, NIST AI RMF, and MITRE ATLAS. Built for red teamers handed AI in scope, blue teamers watching agents deploy faster than detections exist, AppSec engineers who used to own the API and now own a chat window, and developers curious what "prompt injection" looks like when it costs money. No prior AI-security background required.

SpeakerBio: Pavan "pavanreddysec" Reddy

Pavan Reddy is principal developer at Automata LLC, leading FIPS 140-3, FedRAMP ATO, and AI security initiatives. He is an independent AI security researcher and educator focused on making secure AI accessible at scale. He founded QBTrain, a free platform for hands-on AI and AI security education. His peer-reviewed work, published at AAAI, ACM, FLAIRS, HCII, ACSAC, and NeurIPS, spans adversarial ML, prompt injection, and foundation model vulnerabilities. He has delivered 25+ talks and workshops at BSides, OWASP, SquadCon, CAPWIC, ACM SIGCITE, NeurIPS Education, FLAIRS, CVPR 2026 and TechMentor at Microsoft HQ. He holds an MS in CS from George Washington University.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

DEF CON Training - Monday - 08:30-17:30 PDT

Title: Solving Modern Cybersecurity Problems with AI

Tags: DEF CON Training (Paid) (2-day) | DEF CON Training

When: Monday, Aug 10, 08:30 - 17:30 PDT

Where: LVCCW Level 2 W225 (Workshops) - [Map](#)

Description:

SpeakerBio: Michael Glass

No BIO available



[Return to Index](#) - Add to Google

- ics [Calendar](#) file

DEF CON Training - Tuesday - 08:30-17:30 PDT

Title: Solving Modern Cybersecurity Problems with AI

Tags: DEF CON Training (Paid) (2-day) | DEF CON Training

When: Tuesday, Aug 11, 08:30 - 17:30 PDT

Where: LVCCW Level 2 W225 (Workshops) - [Map](#)

Description:

SpeakerBio: Michael Glass

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Source of Truth: A Field Guide for Deep Technical Research

Tags: OWASP Foundation | Creator Talk/Panel

When: Sunday, Aug 9, 12:30 - 12:59 PDT

Where: LVCCW Level 1 Hall 3 1100 (Creator Stage 7) - [Map](#)

Description:

Security research usually starts with one reasonable question and somehow turns into a sea of browser tabs, lost bookmarks, half-read standards, conference talks, vendor docs, AI summaries, and simplified architecture posts with suspiciously perfect rectangles. Finding information is easy. The hard part is learning enough to know which explanation applies, which design decision changes the threat model, and where the simplified diagram quietly skipped the important part.

This talk is a practical field guide for researching deeply technical security topics without getting lost in the noise. We will look at how to approach protocols, standards, system behavior, and implementation details, then trace claims back to primary sources, identify load-bearing assumptions, and turn dense research into something useful for engineers and defenders.

SpeakerBio: Carley “51nk0r5w1m” Fant, OWASP Project contributor, Rabbit Hole explorer

Carley “51nk0r5w1m” Fant is a Platform Engineer focused on AppSec, cloud infrastructure, identity, and software delivery. Her work centers on building secure platform baselines, hardening cloud-native environments, and helping engineering teams ship systems that are usable, observable, defensible, and less cursed by default.

She works at the intersection of platform engineering and application security, with a focus on practical threat modeling, automation, and figuring out where systems actually break once they leave the whiteboard. She is active in the OWASP community and enjoys turning technical rabbit holes into useful takeaways for engineers, defenders, and anyone who has ever opened an RFC, sighed, and kept reading anyway.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Sovereign by Design, Vulnerable by Default

Tags: Policy @ DEF CON | Creator Talk/Panel

When: Friday, Aug 7, 10:00 - 10:59 PDT

Where: LVCCW Level 1 Hall 3 801 (Creator Stage 1) - [Map](#)

Description:

Every major government is now making sovereign AI decisions. Data localization. Domestic cloud mandates. Trusted vendor regimes. Export controls on chips and model weights. Engineers and security teams don't get a vote on whether sovereignty happens — they inherit the architecture it creates. And that architecture has seams. This talk is a security analysis of what sovereignty does to threat models, and what policy designers can do about it. Sovereignty initiatives change architecture. Architecture changes threat models. Policy that ignores this chain creates new vulnerabilities. Policy that understands it can improve resilience — but only if it's designed with the seams in mind.

Speakers: Devin Lynch, Haley Ring

SpeakerBio: Devin Lynch, Paladin Global Institute

Devin Lynch is the Senior Director of the Paladin Global Institute and a former Director for Cyber Policy and Strategy Implementation at the Office of the National Cyber Director (ONCD). He has held key roles in both the private sector and government, including positions at the U.S. House of Representatives, U.S. Senate, and the Departments of Homeland Security and Defense. He is an adjunct professor at the George Washington University's Elliott School of International Affairs and has served in the U.S. Navy Reserve for over 20 years, including combat deployments to Iraq and Afghanistan.

SpeakerBio: Haley Ring, Paladin Global Institute

Haley Ring is the Director at the Paladin Global Institute, where she helps drive initiatives that strengthen national resilience, protect critical infrastructure, and shape the future of emerging technology. She previously served in the Biden-Harris Administration, advising on national security, technology policy, and public engagement as the Advisor for Engagement to the Second Gentleman and as a Special Advisor in the White House Office of the National Cyber Director. Before her White House roles, Haley worked at the Department of Defense in the Office of the White House Liaison. She began her career on the Biden for President campaign and is originally from Newton, Massachusetts. Haley holds a bachelor's degree from the University of Wisconsin–Madison and is based in Washington, D.C.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Aerospace Village - Saturday - 10:00-17:59 PDT

Title: SpaceCOP - Catch Me If You Can

Tags: Aerospace Village | Creator Event/Activity

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 2 700 (Aerospace Village) - [Map](#)

Description:

Think you can hack a spacecraft?

We've deployed a vulnerable Pisat and made the software available ahead of time so you can prove it. Study it, reverse engineer it, find weaknesses, and develop your attack plan before stepping up to the console.

When your turn comes, you'll only have 15 minutes at a time to compromise the spacecraft and achieve a mission objective. There's just one problem, the SpaceCOP, an intrusion detection system based on the Aerospace Corporation's SPARTA matrix, has been deployed. The spacecraft is intentionally hackable - the real challenge is accomplishing your objective without triggering an alert and getting arrested by SpaceCOP.

Earn rewards based on how well you hack and hide from SpaceCOP.

Rules of Engagement: • Recon and vulnerability research before sitting at the terminal are highly encouraged. • You will have 15 minutes at the workstation to execute your attack. • Modifying files, changing registry settings, taking pictures, and other spacecraft effects are fair game. • Do not intentionally wipe, brick, destroy, or otherwise render the system unusable. • No "rm -rf", disk wipes, ransomware, bootloader destruction, or similar actions.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Aerospace Village - Friday - 10:00-17:59 PDT

Title: SpaceCOP - Catch Me If You Can

Tags: Aerospace Village | Creator Event/Activity

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 2 700 (Aerospace Village) - [Map](#)

Description:

Think you can hack a spacecraft?

We've deployed a vulnerable Pisat and made the software available ahead of time so you can prove it. Study it, reverse engineer it, find weaknesses, and develop your attack plan before stepping up to the console.

When your turn comes, you'll only have 15 minutes at a time to compromise the spacecraft and achieve a mission objective. There's just one problem, the SpaceCOP, an intrusion detection system based on the Aerospace Corporation's SPARTA matrix, has been deployed. The spacecraft is intentionally hackable - the real challenge is accomplishing your objective without triggering an alert and getting arrested by SpaceCOP.

Earn rewards based on how well you hack and hide from SpaceCOP.

Rules of Engagement: • Recon and vulnerability research before sitting at the terminal are highly encouraged. • You will have 15 minutes at the workstation to execute your attack. • Modifying files, changing registry settings, taking pictures, and other spacecraft effects are fair game. • Do not intentionally wipe, brick, destroy, or otherwise render the system unusable. • No "rm -rf", disk wipes, ransomware, bootloader destruction, or similar actions.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Aerospace Village - Sunday - 10:00-13:59 PDT

Title: SpaceCOP - Catch Me If You Can

Tags: Aerospace Village | Creator Event/Activity

When: Sunday, Aug 9, 10:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 2 700 (Aerospace Village) - [Map](#)

Description:

Think you can hack a spacecraft?

We've deployed a vulnerable Pisat and made the software available ahead of time so you can prove it. Study it, reverse engineer it, find weaknesses, and develop your attack plan before stepping up to the console.

When your turn comes, you'll only have 15 minutes at a time to compromise the spacecraft and achieve a mission objective. There's just one problem, the SpaceCOP, an intrusion detection system based on the Aerospace Corporation's SPARTA matrix, has been deployed. The spacecraft is intentionally hackable - the real challenge is accomplishing your objective without triggering an alert and getting arrested by SpaceCOP.

Earn rewards based on how well you hack and hide from SpaceCOP.

Rules of Engagement: • Recon and vulnerability research before sitting at the terminal are highly encouraged. • You will have 15 minutes at the workstation to execute your attack. • Modifying files, changing registry settings, taking pictures, and other spacecraft effects are fair game. • Do not intentionally wipe, brick, destroy, or otherwise render the system unusable. • No "rm -rf", disk wipes, ransomware, bootloader destruction, or similar actions.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: SpaceCOP: Houston, We Have an Intrusion

Tags: Aerospace Village | Creator Talk/Panel

When: Saturday, Aug 8, 17:30 - 17:59 PDT

Where: LVCCW Level 1 Hall 3 1103 (Creator Stage 5) - [Map](#)

Description:

Spacecraft are no longer isolated boxes with radios. They are networked, software-defined, mission-critical systems operating in an environment where patching is hard, visibility is limited, and failure can look a lot like an attack. This talk introduces Space Cyber Orbital Protection, or SpaceCOP, a spacecraft intrusion detection system designed to bring threat-informed cyber monitoring onboard the vehicle. SpaceCOP comes in two forms: an open-source version for NASA's Core Flight System, releasing at DEF CON 34, and a closed-source side-loaded architecture intended to integrate with a broader range of spacecraft software environments. The cFS version uses SPARTA's Indicators of Behavior to detect anomalous spacecraft activity. We will walk through why traditional ground-based monitoring is not enough, how spacecraft IDS concepts differ from terrestrial IDS, and how SPARTA-derived behavior indicators can be translated into practical onboard detections. We will also discuss how growing policy pressure, including U.S. national security space guidance and emerging European space cybersecurity requirements, is pushing operators toward onboard intrusion detection and response. Space cyber threats are not theoretical anymore. SpaceCOP is an attempt to move spacecraft defense from "trust the link" to "monitor the vehicle."

SpeakerBio: Brandon Bailey, Aerospace Corporation

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Spotlight: Choose Your Own Adventure with InfoSecMap

Tags: OWASP Foundation | Creator Event/Activity

When: Friday, Aug 7, 11:30 - 11:59 PDT

Where: LVCCW Level 1 Hall 4 1415 (OWASP Foundation) - [Map](#)

Description:

Opportunities in InfoSec are everywhere, but they're often buried across scattered websites, social media posts, or chat channels. Whether it's a local meetup, a CFP deadline, a volunteer opportunity, or the chance to sponsor an initiative, many people and organizations miss out simply because they don't know where to look or find info bloated by pay-to-play noise.

InfoSecMap was created to solve this. It's a free, community-driven platform that brings the global InfoSec ecosystem together in one place. From major conferences to CTFs and grassroots meetups, InfoSecMap helps users explore what's happening by geographic region or focus area and discover where they can connect and contribute.

InfoSecMap is proud to partner with OWASP, bringing together volunteer-led chapters and global events while fostering stronger connections and community growth. We believe open source should mean open access, and we're building the infrastructure to make that real.

SpeakerBio: W. Martín Villalba, OWASP

Martín is an application and product security consultant with over 15 years of industry experience. He founded C13 Security, where he specializes in Secure SDLC, pentesting, and vulnerability management. He is an active member of the InfoSec community, collaborating with local groups and global organizations such as BSides and OWASP. He also built InfoSecMap, an open-access platform for discovering InfoSec events and communities from all around the world.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Spotlight: Choose Your Own Adventure with InfoSecMap

Tags: OWASP Foundation | Creator Event/Activity

When: Sunday, Aug 9, 10:00 - 10:30 PDT

Where: LVCCW Level 1 Hall 4 1415 (OWASP Foundation) - [Map](#)

Description:

Opportunities in InfoSec are everywhere, but they're often buried across scattered websites, social media posts, or chat channels. Whether it's a local meetup, a CFP deadline, a volunteer opportunity, or the chance to sponsor an initiative, many people and organizations miss out simply because they don't know where to look or find info bloated by pay-to-play noise.

InfoSecMap was created to solve this. It's a free, community-driven platform that brings the global InfoSec ecosystem together in one place. From major conferences to CTFs and grassroots meetups, InfoSecMap helps users explore what's happening by geographic region or focus area and discover where they can connect and contribute.

InfoSecMap is proud to partner with OWASP, bringing together volunteer-led chapters and global events while fostering stronger connections and community growth. We believe open source should mean open access, and we're building the infrastructure to make that real.

SpeakerBio: W. Martín Villalba, OWASP

Martín is an application and product security consultant with over 15 years of industry experience. He founded C13 Security, where he specializes in Secure SDLC, pentesting, and vulnerability management. He is an active member of the InfoSec community, collaborating with local groups and global organizations such as BSides and OWASP. He also built InfoSecMap, an open-access platform for discovering InfoSec events and communities from all around the world.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Spotlight: Choose Your Own Adventure with InfoSecMap

Tags: OWASP Foundation | Creator Event/Activity

When: Saturday, Aug 8, 10:30 - 10:59 PDT

Where: LVCCW Level 1 Hall 4 1415 (OWASP Foundation) - [Map](#)

Description:

Opportunities in InfoSec are everywhere, but they're often buried across scattered websites, social media posts, or chat channels. Whether it's a local meetup, a CFP deadline, a volunteer opportunity, or the chance to sponsor an initiative, many people and organizations miss out simply because they don't know where to look or find info bloated by pay-to-play noise.

InfoSecMap was created to solve this. It's a free, community-driven platform that brings the global InfoSec ecosystem together in one place. From major conferences to CTFs and grassroots meetups, InfoSecMap helps users explore what's happening by geographic region or focus area and discover where they can connect and contribute.

InfoSecMap is proud to partner with OWASP, bringing together volunteer-led chapters and global events while fostering stronger connections and community growth. We believe open source should mean open access, and we're building the infrastructure to make that real.

SpeakerBio: W. Martín Villalba, OWASP

Martín is an application and product security consultant with over 15 years of industry experience. He founded C13 Security, where he specializes in Secure SDLC, pentesting, and vulnerability management. He is an active member of the InfoSec community, collaborating with local groups and global organizations such as BSides and OWASP. He also built InfoSecMap, an open-access platform for discovering InfoSec events and communities from all around the world.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Contests - Sunday - 10:00-11:59 PDT

Title: spyVspy 3: Rat Race

Tags: spyVspy 3: Rat Race | Contest

When: Sunday, Aug 9, 10:00 - 11:59 PDT

Where: LVCCW Level 1 Hall 1 206 (spyVspy 3: Rat Race) - [Map](#)

Description:

spyVspy is back, and this year, you're racing.

Embark on a thrilling espionage adventure with spyVspy 3: Rat Race! This contest imagines a world of spy games where contestants employ basic hacking, cryptography, and rogue skills to solve puzzles and uncover hidden caches strategically scattered throughout DEF CON (and beyond).

Challenges leading to the location of hidden caches will be released on a rolling schedule. By solving these challenges and being the first team to reach a cache, you will qualify for a final series of challenges on Saturday afternoon. Not the first? That's okay - you'll still have fun and earn cool spyVspy slabbed cards

spyVspy 3: Rat Race is intended for players of all skill levels. Whether you're a seasoned double-agent or just learning to be a covert operative, you will be able to compete and have fun in this event. Whatever skills you think you're missing can probably be learned on-the-job anyway.

Participant Prerequisites

A laptop would be great, but some puzzles may be solvable on a phone.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Contests - Saturday - 10:00-17:59 PDT

Title: spyVspy 3: Rat Race

Tags: spyVspy 3: Rat Race | Contest

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 206 (spyVspy 3: Rat Race) - [Map](#)

Description:

spyVspy is back, and this year, you're racing.

Embark on a thrilling espionage adventure with spyVspy 3: Rat Race! This contest imagines a world of spy games where contestants employ basic hacking, cryptography, and rogue skills to solve puzzles and uncover hidden caches strategically scattered throughout DEF CON (and beyond).

Challenges leading to the location of hidden caches will be released on a rolling schedule. By solving these challenges and being the first team to reach a cache, you will qualify for a final series of challenges on Saturday afternoon. Not the first? That's okay - you'll still have fun and earn cool spyVspy slabbed cards

spyVspy 3: Rat Race is intended for players of all skill levels. Whether you're a seasoned double-agent or just learning to be a covert operative, you will be able to compete and have fun in this event. Whatever skills you think you're missing can probably be learned on-the-job anyway.

Participant Prerequisites

A laptop would be great, but some puzzles may be solvable on a phone.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Contests - Friday - 10:00-17:59 PDT

Title: spyVspy 3: Rat Race

Tags: spyVspy 3: Rat Race | Contest

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 206 (spyVspy 3: Rat Race) - [Map](#)

Description:

spyVspy is back, and this year, you're racing.

Embark on a thrilling espionage adventure with spyVspy 3: Rat Race! This contest imagines a world of spy games where contestants employ basic hacking, cryptography, and rogue skills to solve puzzles and uncover hidden caches strategically scattered throughout DEF CON (and beyond).

Challenges leading to the location of hidden caches will be released on a rolling schedule. By solving these challenges and being the first team to reach a cache, you will qualify for a final series of challenges on Saturday afternoon. Not the first? That's okay - you'll still have fun and earn cool spyVspy slabbled cards

spyVspy 3: Rat Race is intended for players of all skill levels. Whether you're a seasoned double-agent or just learning to be a covert operative, you will be able to compete and have fun in this event. Whatever skills you think you're missing can probably be learned on-the-job anyway.

Participant Prerequisites

A laptop would be great, but some puzzles may be solvable on a phone.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Aerospace Village - Sunday - 10:00-13:59 PDT

Title: SR-71 Blackbird Badge Challenge

Tags: Aerospace Village | Creator Event/Activity

When: Sunday, Aug 9, 10:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 2 700 (Aerospace Village) - [Map](#)

Description:

Think faster. Fly higher. Stay unseen.

Only the sharpest contenders will earn the limited-edition SR-71 PCB badge, inspired by the legendary Blackbird. Put your technical skills, aerospace knowledge, and analytical thinking to the test in this exclusive challenge. Like the aircraft itself, success demands precision, ingenuity, and the ability to stay one step ahead. Complete the mission and earn your wings.

New challenges launch all weekend long.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Aerospace Village - Friday - 10:00-17:59 PDT

Title: SR-71 Blackbird Badge Challenge

Tags: Aerospace Village | Creator Event/Activity

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 2 700 (Aerospace Village) - [Map](#)

Description:

Think faster. Fly higher. Stay unseen.

Only the sharpest contenders will earn the limited-edition SR-71 PCB badge, inspired by the legendary Blackbird. Put your technical skills, aerospace knowledge, and analytical thinking to the test in this exclusive challenge. Like the aircraft itself, success demands precision, ingenuity, and the ability to stay one step ahead. Complete the mission and earn your wings.

New challenges launch all weekend long.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Aerospace Village - Saturday - 10:00-17:59 PDT

Title: SR-71 Blackbird Badge Challenge

Tags: Aerospace Village | Creator Event/Activity

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 2 700 (Aerospace Village) - [Map](#)

Description:

Think faster. Fly higher. Stay unseen.

Only the sharpest contenders will earn the limited-edition SR-71 PCB badge, inspired by the legendary Blackbird. Put your technical skills, aerospace knowledge, and analytical thinking to the test in this exclusive challenge. Like the aircraft itself, success demands precision, ingenuity, and the ability to stay one step ahead. Complete the mission and earn your wings.

New challenges launch all weekend long.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Stalking the Wily Hacker ... 40 years later

Tags: DEF CON Official Talk

When: Saturday, Aug 8, 13:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 3 903 (Main Track 5) - [Map](#)

Description:

40 years ago today, I tripped over a 75-cent accounting glitch in a Unix system. That tiny clue led to a year-long chase across networks, modem banks, and international borders, ultimately uncovering a crew of German hackers working for the East German Stasi and the Soviet KGB. We had no budget, no roadmap, and no “cyber” anything. We improvised with soldering irons, shell scripts, logbooks, curiosity, and far too much coffee. Let’s revisit the chase – not just to remember, but to ask what changed, what didn’t, and why it still matters.

The Cuckoo’s Egg, Doubleday Books, 1989

Stalking the Wily Hacker, Communications of the ACM May 1988 v31, page 484-497

<https://dl.acm.org/doi/10.1145/42411.42412>

SpeakerBio: Cliff Stoll, Acme Klein Bottle

Cliff graduated from Buffalo Public School #61 with a blue star for good attendance. He’s since fooled around in planetary physics, computer security, and mathematical Klein bottles, with occasional detours into common sense.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Contests - Friday - 10:00-11:59 PDT

Title: StarPWN CTF

Tags: Aerospace Village | STARPWN (Aerospace Village CTF) | Contest

When: Friday, Aug 7, 10:00 - 11:59 PDT

Where: LVCCW Level 1 Hall 2 700 (Aerospace Village) - [Map](#)

Description:

Want to try your hand at hacking satellites, spacecraft and ground control systems? Miss out on Hack-A-Sat? Want to explore the final frontier of cybersecurity?

STARPWN is the official Aerospace Village space hacking CTF! Backdoor flight computers, trojan flight software, exploit CVE's, reverse protocols, and more! During your space hacking journey, you'll learn all about the environmental and operational constraints of space systems, how they affect cybersecurity posture, and impact exploitability.

Register at <https://starpwn.ctfd.io/>

Prizes to the highest finishing team the team that finishes quickest that can make it to the Aerospace Village in person by 1300 local time.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Contests - Saturday - 10:00-11:59 PDT

Title: StarPWN CTF

Tags: Aerospace Village | STARPWN (Aerospace Village CTF) | Contest

When: Saturday, Aug 8, 10:00 - 11:59 PDT

Where: LVCCW Level 1 Hall 2 700 (Aerospace Village) - [Map](#)

Description:

Want to try your hand at hacking satellites, spacecraft and ground control systems? Miss out on Hack-A-Sat? Want to explore the final frontier of cybersecurity?

STARPWN is the official Aerospace Village space hacking CTF! Backdoor flight computers, trojan flight software, exploit CVE's, reverse protocols, and more! During your space hacking journey, you'll learn all about the environmental and operational constraints of space systems, how they affect cybersecurity posture, and impact exploitability.

Register at <https://starpwn.ctfd.io/>

Prizes to the highest finishing team the team that finishes quickest that can make it to the Aerospace Village in person by 1300 local time.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Team Recognition – 100% Effort

WL F-14 F-11-20 11-50 DDE

[illegible]



Title: State Desync as a Weapon: Breaking Transactional Integrity in Payment Systems (ESP)

Tags: La Villa Community | Creator Talk/Panel

When: Friday, Aug 7, 15:30 - 15:59 PDT

Where: LVCCW Level 1 Hall 4 1416 (La Villa Community) Main Stage - [Map](#)

Description:

El Price Tampering no es un simple cambio de parámetro ni un bug, es una falla de arquitectura que permite alterar el valor de una transacción sin romper ningún control tradicional en cualquier sistema que procese pagos, provocando fraude en diferentes industrias y negocios. En esta charla abordaré cómo un atacante modela el flujo de compra y pago completo, identifica puntos de desincronización entre cliente, backend y pasarela, y explota la ausencia de invariantes de negocio server-side para manipular el valor final de una transacción sin necesidad de CVEs, exploits ni malware. Basado en una investigación propia con casos reales autorizados y anonimizados en entornos de banca, retail y fintech en LATAM, presentaré una taxonomía de tres patrones de ataque recurrentes y un modelo defensivo concreto llamado FinSecure, sustentado en el principio del backend soberano, donde el precio nunca puede nacer fuera del servidor. La audiencia se irá con una visión diferente del problema y herramientas accionables para detectarlo y eliminarlo por diseño.

SpeakerBio: Santiago Sepúlveda Veliz, Pentester / Security Researcher - AppSec & Transactional Integrity

Mi nombre es Santiago Sepúlveda Veliz, hoy en día me desempeño como Pentester y Security Researcher especializado en AppSec e integridad transaccional, con 3 años de experiencia profesional realizando evaluaciones de seguridad en aplicaciones web, móviles, APIs y entornos Active Directory para clientes enterprise en Latinoamérica. Actualmente me desempeño en TRUSTTECH Cybersecurity, enfocado en seguridad de plataformas de pago y lógica de negocio. Cuento con las certificaciones OSCP+ (Offensive Security) y CRT0 (Zero-Point Security). Soy speaker aceptado en PyCon Latam 2026. He asistido a DEF CON 32 y 33, RootedCON Panamá, Ekoparty Argentina y el Congreso 8.8 Chile. Soy creador de contenido técnico de ciberseguridad en YouTube bajo el alias Y4nbow con más de 3.700 suscriptores.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

The Diana Initiative - Saturday - 11:00-11:59 PDT

Title: Stay Sharp: Navigating Pen Testing and Bug Bounty in an AI-Driven World

Tags: The Diana Initiative | Creator Talk/Panel

When: Saturday, Aug 8, 11:00 - 11:59 PDT

Where: LVCCW Level 2 W209 (Diana Initiative) - [Map](#)

Description:

AI is no longer on the horizon — it's already in our workflows, our attacker toolkits, and our vulnerability landscapes. For penetration testers and bug bounty professionals, the skills that got us here won't be enough to keep up.

This session is built for the full cyber community — students exploring careers, professionals breaking in, and program leaders rethinking their approach. We'll cover the training and certifications worth investing in, how to identify and close skill gaps, and why community, mentorship, and peer networks remain our most important growth asset. For those leading teams, we'll tackle a harder question: how do you build a learning culture that keeps up with change without burning people out? The AI field is moving fast. We have to move with it.

SpeakerBio: Dana Pirvu, Senior Manager of Product and Software Security at Adobe

Dana Pirvu is a Senior Manager of Product and Software Security at Adobe, overseeing the Penetration Testing and Bug Bounty programs. In her role, Dana drives continuous product security testing efforts and partners with external researchers to proactively identify vulnerabilities across Adobe's products and services, translating security findings into actionable insights for engineering and leadership teams.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Stealing at the Speed of Light: The Anatomy of a Real Relay Attack tool

Tags: Car Hacking Village | Creator Talk/Panel

When: Sunday, Aug 9, 11:30 - 11:59 PDT

Where: LVCCW Level 1 Hall 3 801 (Creator Stage 1) - [Map](#)

Description:

Passive Keyless Entry and Start (PKES) systems allow a driver to unlock and start a vehicle without any deliberate interaction with the key, relying instead on an automated radio-frequency exchange between the key fob and the car whenever the two are in close proximity. This talk begins by explaining the operating principles of PKES and the challenge-response communication that links the fob to the vehicle, establishing the implicit trust assumption — that proximity equals legitimacy — on which the system depends. I will then describe the process of sourcing and operating a real, commercially available relay attack tool, illustrated with a demonstration video of the attack carried out against a vehicle, before presenting a research deep-dive into how the tool is constructed and how it relays the signal across distance to defeat the proximity assumption. Finally, I will discuss mitigation strategies that aim to close the gap the attack exploits.

SpeakerBio: Robbie Galfrin, PlaxidityX

Robbie Galfrin is an embedded security researcher with over 12 years of experience in hardware and software vulnerability research and exploitation. At PlaxidityX since 2017, his main focus has been low-level and hardware attacks on automotive ECUs, operating systems, and communication interfaces. Holds an MSc in Electrical Engineering from Tel Aviv University.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Step Zero: Identifying the Quantum Attack Surface in Critical Infrastructure

Tags: Crypto & Privacy Village | Creator Talk/Panel

When: Friday, Aug 7, 15:45 - 16:30 PDT

Where: LVCCW Level 1 Hall 3 801 (Creator Stage 2) - [Map](#)

Description:

Every wire transfer, banking session, API transaction, and SWIFT message depends on RSA and ECC cryptography that a sufficiently powerful quantum computer will eventually break with Shor's algorithm. That part is well known.

The real problem is that most financial institutions have no idea where that cryptography actually lives.

RSA and ECC are buried inside banking APIs, certificate hierarchies, SWIFT authentication, third-party software dependencies, mobile applications, HSM integrations, and legacy infrastructure that was never designed for crypto-agility. Most organizations cannot inventory it, prioritize it, or migrate what they cannot find.

This talk focuses on the real quantum attack surface inside financial infrastructure, not the theoretical one.

We examine two high-impact cryptographic systems hiding in plain sight: • SWIFT authentication infrastructure securing interbank trust • TLS certificate hierarchies protecting banking sessions, APIs, and payment platforms

Then we move from theory to operational reality.

Using open-source Cryptographic Bill of Materials (CBOM) tooling, we demonstrate how to identify quantum-vulnerable cryptography across financial systems, uncover hidden RSA and ECC dependencies, and build usable cryptographic inventories that defenders can actually operationalize.

We also examine why this is a current collection problem, not a future one. Nation-state adversaries are already harvesting encrypted financial traffic and long-lived sensitive data for future decryption under harvest-now, decrypt-later (HNDL) strategies. Your encrypted traffic does not need to be decrypted today to become valuable tomorrow.

The talk includes: • Live CBOM generation using IBM CBOMkit • Discovery of hidden RSA and ECC dependencies inside financial infrastructure • Practical guidance for prioritizing post-quantum migration

Not policy. Not hype. Tools, cryptographic visibility, and attack surface.

Speakers: Dr. Katrina Rosseini, Dr. Allan Friedman

SpeakerBio: Dr. Katrina Rosseini

Dr. Katrina Rosseini is a strategist at the intersection of cybersecurity, quantum computing, PQC, and AI, advising policymakers and stakeholders on U.S. positioning in global technology competition with national security at the core. She is the Founder of KRR Ventures Advisory and leads Critical Effect California, a forum that convenes policymakers, infrastructure operators, and private-sector leaders on cybersecurity and operational risk. As Chair of the Civilian Reserve (CR-ISAC), she supports a national network of veterans and civilian experts strengthening the resilience of critical infrastructure. A Visiting Fellow at the National Security Institute, Dr. Rosseini focuses on quantum risk and the post-quantum transition. She has briefed the nation's largest public pension fund and contributed to congressional and United Nations forums. She developed the QUEEN Framework, a quantum governance model integrating cryptographic risk into board-level decision-making, and SECUREGRID, a methodology for prioritizing vulnerabilities in operational technology. Her commentary has appeared in Forbes, S&P Global, and Fast Company, among others. She holds a Doctor of Engineering from George Washington University and an MBA in Finance.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

The Diana Initiative - Friday - 13:00-13:59 PDT

Title: Stigma is stupid: Let's talk about recovery, mental wellness, and hard stuff without making it awkward

Tags: The Diana Initiative | Creator Talk/Panel

When: Friday, Aug 7, 13:00 - 13:59 PDT

Where: LVCCW Level 2 W209 (Diana Initiative) - [Map](#)

Description:

This will be a discussion group about how we talk (or don't talk) about recovery, sobriety, mental wellness, burnout, grief, and other hard human things in cybersecurity spaces. Silence feeds stigma, but not everyone knows how to start the conversation safely or supportively. We'll discuss language, boundaries, allyship, and ways to create community without turning every vulnerable conversation into a TED Talk or therapy session.

SpeakerBio: Jennifer VanAntwerp, ABM Manager at StrongDM

Jen VanAntwerp is the founder of Sober in Cyber, a nonprofit on a mission to provide alcohol-free events and community-building opportunities for sober individuals working in cybersecurity. She is passionate about breaking the stigma of addiction recovery and is profoundly driven to increase the number of professional networking events that don't revolve around alcohol. Jen is also the ABM manager at StrongDM, the Zero Trust privileged access platform. When she's not developing marketing strategies or running her nonprofit, Jen enjoys volunteering, sewing, and tinkering with her beloved '65 Ranchero.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Stop Chasing Domain Admin: Designing Red Team Exercises That Matter

Tags: Red Team Village | Misc

When: Saturday, Aug 8, 13:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 1 309 (Red Team Village) Workshop Stage 2 - [Map](#)

Description:

You got domain admin. No alerts fired. The red team “won.” But did the exercise actually test anything that matters?

Red team engagements are often evaluated based on familiar outcomes such as full compromise, stealth, or the use of novel techniques. While these may demonstrate operator skill, they frequently fail to answer the question the engagement was meant to address.

This session challenges a common industry pattern: optimizing for technical achievement instead of meaningful outcomes. When red teams focus on getting domain admin or remaining undetected as primary goals, exercises often measure attacker creativity rather than organizational resilience.

Through a short presentation and an interactive, drop-in workshop, participants will learn how to design red team exercises around clear defensive questions. Attendees will build components of real-world engagements by defining objectives, selecting starting conditions, choosing techniques, and determining meaningful success metrics.

The workshop is structured as a series of modular steps, allowing participants to join at any time and engage at their own pace. Whether participants spend five minutes or the full session, they will leave with a practical framework for planning red team operations that produce actionable insight.

If you’ve ever seen a red team achieve full compromise and still felt like the exercise didn’t answer the right questions, this session is for you.

You will leave with a clearer understanding of what red teaming is supposed to accomplish, and a practical way to design engagements that deliver meaningful results.

SpeakerBio: Billy Giles

Billy Giles is an Offensive Security leader and practitioner who specializes in red/purple teaming and network penetration testing. With a deep passion for understanding adversary behaviors, he helps organizations across a multitude of industries assess their security postures, identify and remediate vulnerabilities, and build stronger defenses by thinking like an attacker.

Billy is also the creator of Thinking Offensively. Through this project he examines offensive security strategy topics to help cybersecurity leaders anticipate threats and inform decision making, while also providing tools, playbooks, and techniques that red teams can apply directly to their work. His mission is to bridge strategy and execution to help organizations think offensively and stay ahead of evolving threats.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

DEF CON Training - Monday - 08:30-17:30 PDT

Title: Strategic AI Penetration: Mastering Offensive Techniques for LLMs

Tags: DEF CON Training (Paid) (2-day) | DEF CON Training

When: Monday, Aug 10, 08:30 - 17:30 PDT

Where: LVCCW Level 2 W233 (Workshops) - [Map](#)

Description:

Speakers: Marek Zmysłowski, Konrad Jędrzejczyk

SpeakerBio: Marek Zmysłowski

No BIO available

SpeakerBio: Konrad Jędrzejczyk

No BIO available

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

DEF CON Training - Tuesday - 08:30-17:30 PDT

Title: Strategic AI Penetration: Mastering Offensive Techniques for LLMs

Tags: DEF CON Training (Paid) (2-day) | DEF CON Training

When: Tuesday, Aug 11, 08:30 - 17:30 PDT

Where: LVCCW Level 2 W233 (Workshops) - [Map](#)

Description:

Speakers: Marek Zmysłowski, Konrad Jędrzejczyk

SpeakerBio: Marek Zmysłowski

No BIO available

SpeakerBio: Konrad Jędrzejczyk

No BIO available

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Strategic Resistance: How a Global Network is Fighting the Spyware Industry -

Tags: Policy @ DEF CON | Creator Talk/Panel

When: Sunday, Aug 9, 11:00 - 11:59 PDT

Where: LVCCW Level 2 W210-211 (Policy Village) - [Map](#)

Description:

For years, the commercial spyware industry – which sells software to hijack devices – has operated in a "gray market" with near-total impunity. That changed on February 26, 2026, when an Athens court sentenced executives of Intellexa to maximum prison terms – the first criminal conviction of spyware vendors. This was not an isolated event, but the result of a coordinated, multi-year effort by a diverse network of forensic researchers, legal advocates, and civil society organizations. From the \$167M civil judgment against NSO Group to the closure of critical zero-day flaws in global messaging platforms, the tide is turning against mercenary surveillance. This session explores how this decentralized network supported by the Spyware Accountability Initiative (SAI) is dismantling the spyware business model. We will move beyond individual exploits to analyze the “policy infrastructure that makes technical security research impactful. We’ll show how technical discovery turns into legal and financial consequences for spyware companies. We will also detail how the SAI pooled fund model coordinates resources across organizations like Citizen Lab, the Knight First Amendment Institute, and regional threat labs on every continent. Attendees will gain an inside look at how this initiative operates, how it prioritizes high-impact

Speakers: Michael Brennan, Nadine Farid Johnson, Rebekah Brown

SpeakerBio: Michael Brennan, Spyware Accountability Initiative

Michael Brennan works at the intersection of technology, civil society, and philanthropy, helping build the funding and coordination strategies that make accountability efforts possible. His work focuses on translating between technical researchers, legal advocates, and policy actors to support effective responses to digital threats, including commercial spyware. He has helped shape collaborative approaches to complex public-interest technology challenges and is particularly interested in the often-invisible infrastructure (funding models, networks, and strategy) that turns technical discovery into meaningful consequences for powerful actors. He brings a cross-disciplinary perspective on how to make resistance to surveillance more durable, coordinated, and effective. He holds a PhD in Computer Science.

SpeakerBio: Nadine Farid Johnson, Knight First Amendment Institute

Nadine Farid Johnson is the inaugural policy director of the Knight First Amendment Institute at Columbia University. She is responsible for the Institute’s policy and advocacy efforts, leading engagement with U.S. government and other officials to advance the Institute’s policy objectives. A former U.S. diplomat and professor of law and political science, Farid Johnson is a frequent media contributor, with commentary appearing in The New York Times, The Wall Street Journal, The Atlantic, World Politics Review, Al Jazeera, The Hill, The Daily Beast, NPR, and other national and international publications. She has also appeared on outlets including PBS and CNN International.

SpeakerBio: Rebekah Brown

Rebekah Brown is a senior researcher at the Citizen Lab focussing on targeted threats against civil society. She has over 20 years of experience in threat intelligence and analysis. Before joining the Citizen Lab, Rebekah worked at Apple, where she focused on complex threat models and helped design and implement features for individuals at increased risk for stalking, harassment, and abuse. She is a trained network warfare analyst and previously served as operations chief of a U.S. Marine Corps cyber unit and a U.S. Cyber Command training and exercise lead. Rebekah is a published author on intelligence-driven incident response, and co-author of the SANS course on cyber threat intelligence.



Title: Strengthening the CVE Ecosystem (Seating is limited to 50 Participants)

Tags: Policy @ DEF CON | Creator Interactive Talk/Panel

When: Friday, Aug 7, 14:00 - 15:30 PDT

Where: LVCCW Level 2 W210-211 (Policy Village) - [Map](#)

Description:

CVE is core infrastructure for vulnerability management, but it's under real strain. The volume and complexity of vulnerabilities keep rising, while the systems, tooling, and coordination models behind CVE haven't kept pace. This was true prior to the extensive use of AI to identify vulnerabilities and has only grown more acute. At the same time, governments and industry are relying on CVE data more than ever to drive security decisions, and there are concerns about whether current funding models are sustainable. This roundtable brings together the people who actually work with CVE (researchers, open-source maintainers, vendors, and policymakers) to talk frankly about what's breaking and what needs to change. We'll focus on three areas: gaps in CVE data and infrastructure, where automation and AI can realistically help, and how to build sustainable public-private support for the ecosystem - all with the goal of identifying concrete policy steps that could improve CVE over the next 12-24 months. This discussion would feed into a policy paper making recommendations for policymakers, published by the Center for Cybersecurity Policy and Law.

Seating is limited to the first 50 participants in order to facilitate interactive discussion.

Speakers: John Banghart, Elizabeth Eigner, Lisa Olsen, Lindsey Cerkovnik

SpeakerBio: John Banghart, Center for Cybersecurity Policy & Law

John Banghart leverages his significant federal government and private sector experience in cybersecurity to navigate issues related to risk management, government policy, standards and regulatory compliance, and incident management. He has successfully led efforts to address significant and high-profile cybersecurity issues within major government programs and institutions while facing complex legal, technical, and political circumstances. From 2013 to 2015, John played a key role in developing the Obama administration's cybersecurity and technology policy as the National Security Council's director for federal cybersecurity. He led policy, technical, and process efforts to reduce cybersecurity risk and improve metrics and measurement for all civilian, military, and intelligence community agencies. He served as a primary advisor on cybersecurity incidents and preparedness and led the National Security Council's efforts to address significant cybersecurity incidents, including those at OPM and the White House, among others. He also spent several years at the National Institute of Standards and Technology (NIST), both as a cybersecurity researcher and in the Office of the Undersecretary of Commerce for Standards and Technology. John also worked as a senior cybersecurity advisor for the Centers for Medicare and Medicaid Services, providing leadership to the cybersecurity preparations for the Healthcare.gov website.

SpeakerBio: Elizabeth Eigner, Microsoft

Elizabeth Eigner is a Senior Manager on Microsoft's Global Cybersecurity Policy team, where she leads Microsoft's vulnerability policy portfolio, overseeing efforts to develop and implement strategies that address vulnerability management both in the United States and globally. She represents Microsoft on the Hacking Policy Council, where she works collaboratively with industry leaders and policymakers to advance responsible cybersecurity and strengthen the frameworks that underpin software security worldwide. Elizabeth also leads initiatives aimed at creating and enhancing national cyber strategies in countries around the world. She works closely with governments and stakeholders to strengthen policy frameworks and promote resilient cybersecurity practices globally. Elizabeth also leads Microsoft's Advancing Regional Cybersecurity (ARC) initiative, focusing on improving incident response capabilities and cyber capacity building in the Global South. Previously, she served as Microsoft's representative on the Cloud Service Provider Advisory Board (CSP-AB), contributing to FedRAMP public policy discussions and best practices for cloud security. Before joining Microsoft, Elizabeth worked at The Washington Technology Industry Association to enhance Washington State's innovation ecosystem. At MIT

Solve, she collaborated with tech-based social entrepreneurs on solutions fostering digital inclusion and equitable economic opportunity. She holds a B.S. in Political Science from Northeastern University, with concentrations in Law and International Security.

SpeakerBio: Lisa Olsen, Principal Security Release Program Manager at Microsoft

Lisa Olson is a Principal Security Release Program Manager at Microsoft, where she has led the Patch Tuesday release process since 2013. A member of the CVE Board since 2018, Lisa is a passionate advocate for improving vulnerability communication through automation and machine-readable formats. Her work focuses on transforming how security information is shared to help organizations respond faster and more effectively.

SpeakerBio: Lindsey Cerkovnik, CISA

Lindsey Cerkovnik is the Chief of CISA's Vulnerability Response & Coordination (VRC) Branch. Her team is responsible for CISA's Coordinated Vulnerability Disclosure (CVD) process, the Known Exploited Vulnerabilities (KEV) catalog, and CISA's Stakeholder Specific Vulnerability Categorization (SSVC) process. Lindsey and her team help to maintain, support, and advance the global vulnerability ecosystem by funding and overseeing the CVE and CVE Numbering Authority (CNA) programs, leading the production and dissemination of machine-readable vulnerability enrichment information, and engaging in valuable technical collaboration with the vulnerability research community.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

.EDU Community - Friday - 12:00-12:59 PDT

Title: Student-Run Cyber Clubs - Why They Matter & Digital Playgrounds

Tags: .EDU Community | Creator Talk/Panel

When: Friday, Aug 7, 12:00 - 12:59 PDT

Where: LVCCW Level 1 Hall 4 1418 (.EDU Community) - [Map](#)

Description:

SpeakerBio: Steven "Stengo" Ngo

Steven Ngo is a third-year Ph.D. student in Software Engineering at the University of California, Irvine, advised by Associate Professor Joshua Garcia, with research interests in software engineering & security education and software security. Ngo studies student-run organizations (e.g., cyber clubs) to understand their perspectives and motivations in providing informal modalities of peer-to-peer education, which facilitate the development of educational collaborations, frameworks, and tools to support such organizations.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Supertooth: Wideband Bluetooth Observation with a HackRF

Tags: Radio Frequency Village | Creator Talk/Panel

When: Friday, Aug 7, 16:30 - 16:55 PDT

Where: LVCCW Level 1 Hall 1 409 (Radio Frequency Village) - [Map](#)

Description:

Modern Bluetooth environments are inherently difficult to observe. Classic piconets frequency-hop 1,600 times per second, forcing sniffers to choose between tracking a single connection or losing visibility across the spectrum. Supertooth is an open-source, C-based SDR platform built on the HackRF that eliminates this tradeoff. Instead of traditional hop-following, it captures a fixed 20 MHz slice of the 2.4 GHz band, fanning the raw IQ stream into parallel per-channel demodulation workers. This approach provides simultaneous, real-time visibility into up to 20 BR/EDR channels at once.

Each worker runs an independent GFSK demodulation pipeline powered by liquid-dsp, feeds decoded bitstreams into access-code correlators, and hands matching frames to libbtbb for UAP recovery and HEC-based clock tracking, all without needing to know a piconet's future frequency hops. Supertooth also features a hybrid mode that decodes a Bluetooth low energy advertising channel concurrently from the same 20 MHz stream, exposing advertising data alongside classic piconet activity in a unified view. Per-role RSSI separation further allows researchers to distinguish central and peripheral transmission patterns from passive observation alone.

This talk walks through the tool end-to-end, detailing how Supertooth improves on traditional single-channel workflows like those used by the Ubertooth. We will demonstrate the platform live, discuss current recovery capabilities and the limitations of passive clock tracking, and outline a roadmap for future development. The project is open-source, and the build requires only a HackRF, libhackrf, liquid-dsp, and libbtbb.

SpeakerBio: Dalton Cox, Security Researcher at Skinny R&D

Dalton Cox is a security researcher at Skinny Research & Development in Huntsville, Alabama, where he develops applied AI and various tooling for cybersecurity operations. He is concurrently studying Computer Engineering at the University of Alabama in Huntsville. In his spare time, he plays strategy and card games, experiments with audio gear, and dabbles in a variety of musical instruments.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Supply Chain Isn't Just Dependencies Anymore: Defending Developers, Tooling, and Builds

Tags: Intermediate | AppSec Village | Creator Workshop

When: Saturday, Aug 8, 13:15 - 15:59 PDT

Where: LVCCW Level 1 Hall 2 604 (Appsec Village) Classroom - [Map](#)

Description:

Software supply chain attacks are no longer limited to outdated, vulnerable, or compromised open-source libraries. Today, attackers target developers directly by poisoning package ecosystems, abusing build pipelines, exploiting IDE extensions, and increasingly manipulating AI-assisted coding workflows.

In this interactive two-hour workshop, Tanya Janca will break down the modern software supply chain, what has changed, and why traditional DevSecOps approaches are no longer enough. Participants will learn how attackers think, how developer behavior is being exploited, and what practical controls actually reduce risk (without slowing teams down too much!).

The session covers the next evolution of DevSecOps tooling and practices, explores emerging threats including AI-generated dependency confusion, and provides concrete guidance for securing the developer environment, from IDEs to sandboxes to CI systems.

SpeakerBio: Tanya "SheHacksPurple" Janca

Tanya Janca, known online as SheHacksPurple, is the best-selling author of Alice and Bob Learn Secure Coding and Alice and Bob Learn Application Security. She is the CEO of She Hacks Purple Consulting, where she delivers high-impact, live, secure-coding training for engineering teams. She is also the host of DevSec Station Podcast.

Over 29 years in the industry Tanya has received numerous awards, spoken at events worldwide, and built a reputation as one of the most approachable and influential voices in application security. She has trained thousands of developers and security practitioners through her academies and live programs. Her experience includes counter-terrorism work, leading security for the 42nd Canadian federal election, as well as building and securing a vast range of applications. Today, she is recognized internationally as a leading authority on the security of software.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Policy @ DEF CON - Saturday - 13:00-13:59 PDT

Title: Surprise Session - Check Hacker Tracker

Tags: Policy @ DEF CON | Creator Talk/Panel

When: Saturday, Aug 8, 13:00 - 13:59 PDT

Where: LVCCW Level 2 W210-211 (Policy Village) - [Map](#)

Description:



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Tactical Advocacy: Panel & Peer Sessions with EFF

Tags: Policy @ DEF CON | Creator Interactive Talk/Panel

When: Sunday, Aug 9, 12:30 - 13:59 PDT

Where: LVCCW Level 2 W210-211 (Policy Village) - [Map](#)

Description:

Speakers: Thorin Klosowski, Cooper "Cybertiger" Quintin, Alexis Hancock, Cindy Cohn, Rory Mir

SpeakerBio: Thorin Klosowski, Electronic Frontier Foundation

Senior Security and Privacy Activist, works on Surveillance Self-Defense, providing practical security and privacy guidance for a variety of threat models and across a breadth of consumer electronics.

SpeakerBio: Cooper "Cybertiger" Quintin, Board Member at Open Archive

Cooper Quintin is a security researcher and senior public interest technologist with the EFF Threat Lab. research fellow with Citizen Lab, adviser to CoRD Research and Design, and board member of Open Archive. He has worked on projects including Rayhunter, Privacy Badger, Canary Watch, and analysis of state sponsored malware campaigns such as Dark Caracal. Cooper has given talks about security research at prestigious security conferences including Black Hat, DEFCON, Enigma Conference, and ReCon about issues ranging from IMSI Catcher detection to fem tech privacy issues to newly discovered APTs. He has also been published or quoted in publications including: The New York Times, Reuters, NPR, CNN, and Al Jazeera. Cooper has given security trainings for activists, non profit workers, and vulnerable populations around the world. He previously worked building websites for nonprofits, including Greenpeace, Adbusters, and the Chelsea Manning Support Network. Cooper was also an editor and contributor to the hacktivist journal, "Hack this Zine." In his spare time he enjoys making music, visualizing a solar-punk communitarian future, and playing with his kids.

SpeakerBio: Alexis Hancock, Director of Engineering at Electronic Frontier Foundation

Alexis works to keep the networks strong and encrypted by managing the Certbot project. As well as ensuring EFF open source tools for the public are well supported. She researches an intersection of issues on digital rights, encryption, and consumer technology. She believes in an open and equitable web through encouraging expansion of security by default, bridging engineers and security research, and advocating for better and stronger tech policy and standards.

SpeakerBio: Cindy Cohn, Executive Director at Electronic Frontier Foundation

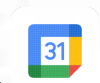
Cindy Cohn is the Executive Director of the Electronic Frontier Foundation. From 2000-2015 she served as EFF's Legal Director as well as its General Counsel. Ms. Cohn first became involved with EFF in 1993, when EFF asked her to serve as the outside lead attorney in *Bernstein v. Dept. of Justice*, the successful First Amendment challenge to the U.S. export restrictions on cryptography. Ms. Cohn is the author of the professional memoir, called *Privacy's Defender* published by MIT Press in March, 2026. She is also the co-host of EFF's award-winning podcast, *How to Fix the Internet*.

--

Cohn first became involved with EFF in 1993, when EFF asked her to serve as the outside lead attorney in *Bernstein v. Dept. of Justice*, the successful First Amendment challenge to the U.S. export restrictions on cryptography. She served as EFF's Legal Director as well as its General Counsel from 2000 through 2015, and she has served as Executive Director since then. She also has co-hosted EFF's award-winning "How to Fix the Internet" podcast, which recently concluded its sixth season. Her professional memoir covering her time at EFF, *Privacy's Defender: My Thirty-Year Fight Against Digital Surveillance*, was published earlier this year by MIT Press.

SpeakerBio: Rory Mir, Electronic Frontier Foundation

Director of Open Access & Tech Community Engagement, where they drive advocacy on access to knowledge, emerging technologies, and user autonomy. They also partner with community builders, experts, and other EFF volunteers to fostering strategic coordination and knowledge sharing.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Tag, You're It: Authorization Traps in AWS ABAC

Tags: Cloud Village | Creator Talk/Panel

When: Sunday, Aug 9, 10:00 - 10:40 PDT

Where: LVCCW Level 3 W313 (Cloud Village Talks) - [Map](#)

Description:

AWS Attribute-Based Access Control (ABAC) is gaining popularity for good reason: it scales well, minimizes policy duplication, and aligns with dynamic cloud environments. However, it can expand the attack surface in unexpected ways. In AWS, ABAC often relies on tags and attributes whose semantics are easier to misunderstand than most practitioners realize. Those semantics determine whether a policy actually enforces the intended boundary, or quietly creates a new attack surface. In this talk, we present a taxonomy of authorization traps in AWS ABAC: recurring patterns where policies look correct but do not behave as expected. These traps arise from ambiguous documentation, non-obvious IAM evaluation rules, service-specific behavior, and edge cases. Different as they may be, they often lead to the same result: a broken security boundary. This talk is for anyone building, reviewing, or attacking access control in AWS - from cloud security practitioners and IAM engineers to red teamers. Expect real policy examples, common failure patterns, and practical techniques you can apply directly in your own environments, with takeaways relevant to almost any AWS setup.

SpeakerBio: Itay Saraf

Itay Saraf is a Senior Cloud Security Researcher at CrowdStrike. He has a background of offensive security, and worked as a red teamer targeting enterprise environments around the world, including multiple Fortune 500 companies. Today, he brings that offensive mindset to cloud and AI research, focusing on exposing real-world threats in modern cloud infrastructure.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Recon Village - Saturday - 13:00-13:30 PDT

Title: Tag, You're It: Physical Tracking Tech, Defense, and How to DIY Your Own

Tags: Recon Village | Creator Talk/Panel

When: Saturday, Aug 8, 13:00 - 13:30 PDT

Where: LVCCW Level 1 Hall 3 801 (Creator Stage 2) - [Map](#)

Description:

We live in an era where our location data is constantly harvested, but what happens when the tracking becomes physical? From the clandestine beacons of the Cold War to the consumer-grade AirTags tucked into backpacks today, physical tracking technology has become incredibly cheap, accessible, and pervasive.

In this talk, we will trace the evolution of physical tracking tech, analyze how modern implementations exploit wireless protocols like BLE, cellular, and GPS, and discuss practical defense strategies to detect and neutralize unwanted eyes.

Finally, we will demystify the threat by turning the tables: demonstrating how to build and deploy a fully functional, budget-friendly tracking beacon using off-the-shelf DIY hardware.

Attendees will leave with a deep understanding of the tracking landscape and the knowledge required to both defend against and build these systems.

SpeakerBio: Eddie Miro, Operations Manager - HackerHaus Security Solutions

Cybersecurity Professional & Creator | Community Builder | Speaker

I build communities, break into systems (legally), and share what I learn along the way. With over a decade of deep involvement in the hacker community, my work spans public speaking, content creation, and technical contributions.

Key Highlights:

Speaking & Community: Featured speaker at 30+ conferences (including DEF CON 27 SE Village) and dedicated volunteer at 25+ events. Former DEF CON Goon.

Media & Content: Hosted Simply Social Engineering, guest on 20+ podcasts, and published writer in 2600 Magazine.

Projects & Ventures: Founder of Octopus Game. Contributor to Black Hills Information Security's Backdoors & Breaches.

Always building and still punk. Let's connect.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Misc - Friday - 15:30-16:30 PDT

Title: tAIrot Readings

Tags: Women in Security and Privacy (WISP) | Creator Event/Activity

When: Friday, Aug 7, 15:30 - 16:30 PDT

Where: LVCCW Level 1 Hall 4 1303 (Women in Security and Privacy (WISP) Community) - [Map](#)

Description:

Curious about what the cards have in store for you? For a suggested donation, WISP Board Chair Alyssa Coley give you an AI-assisted tarot reading! Drop by for a fresh perspective on your burning questions, blending ancient symbolism with modern tech to offer personalized, reflective insights for your journey.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Hackers.town - Saturday - 12:00-12:59 PDT

Title: Take Back Your Memories

Tags: Hackers.town | Creator Talk/Panel

When: Saturday, Aug 8, 12:00 - 12:59 PDT

Where: LVCCW Level 1 Hall 4 1420 (Hackers.town) - [Map](#)

Description:

SpeakerBio: Patrick Sliney, Tech Reclaimers

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Taking on the Dark Fleet... in Cyberspace!

Tags: DEF CON Official Talk

When: Sunday, Aug 9, 13:30 - 13:59 PDT

Where: LVCCW Level 1 Hall 3 906 (Main Track 3) - [Map](#)

Description:

In 2026, the US led what would become an international crackdown on Dark Fleet (sometimes called Shadow/Ghost Fleet): vessels that illegally transport sanctioned oil or other cargo. Little known to the public, Coast Guard Cyber Command was deploying its Cyber Protection Teams (CPTs) onboard these vessels to assure the security & safety of these vessels in cyber space. This talk provides a rare look at the US cyber operators deploying on Dark Fleet Tankers, the danger these vessels pose, and lessons learned from these boardings.

US Coast Guard Cyber Trends in the Maritime Environment 2025 (URL pending release) The Global Oil Tanker Market: An Overview as It Relates to Sanctions (<https://www.congress.gov/crs-product/R47962>)

Speakers: Kenneth Miltenberger, Shane Cancilla

SpeakerBio: Kenneth Miltenberger, US Coast Guard / 2003 Cyber Protection Team

Commander Kenny Miltenberger currently serves as the first Commanding Officer of the 2003 Cyber Protection Team (CPT) in Alameda, CA. He is responsible for protecting the nation's Marine Transportation System in cyberspace by conducting hunt, assess, and incident response operations. His team is the Coast Guard's newest CPT and the only CPT geographically detached from Coast Guard Cyber Command (CGCYBER). He led the DEFCON 33 presentation, "From Shanghai to the Shore: The Silent Threat in Global Shipping".

Kenny recently completed an assignment where he founded the Coast Guard's Red Team and ran the Coast Guard's Blue Team. During that tour he founded CGCYBER's educational phishing capability, led cyber Opposing Forces for a major multinational exercise, and oversaw over 100 Red and Blue Team missions. Other notable positions include his work as an engineer for the U.S. Navy's Naval Sea Systems Command, where he was a developer on a shipboard cyber security platform.

Kenny has a BS in Electrical Engineering from the Coast Guard Academy and an MS Electrical Engineering from University of Maryland (UMD) College Park.

Kenny has also worked as part-time faculty at UMD College Park, where he taught Binary Exploitation in their Cyber Masters Program. Industry certifications include OSCP, GXPN, GCPN, GREM, and more

SpeakerBio: Shane Cancilla, US Coast Guard / 2003 Cyber Protection Team

Shane Cancilla is the Network Engineer for the 2003 Cyber Protection Team in Alameda, CA, focused on building and integrating tools for assessment, incident response, and threat hunting missions across Marine Transportation System and IT/OT/ICS environments. His work spans the engineering and deployment of sensors across complex networks and supporting mission-critical operations as a network analyst.

He has previously worked with organizations including Lawrence Livermore and Lawrence Berkeley National Laboratories, where he supported high performance computing and virtualized network environments.

Shane holds a B.S. in Computer Science from California State University, East Bay, along with CCNA and GCIH certifications.



Title: Talkers Without Borders: Worldwide Free Speech without an Internet Connection

Tags: DEF CON Official Talk | Demo | Tool

When: Sunday, Aug 9, 14:00 - 14:30 PDT

Where: LVCCW Level 1 Hall 3 906 (Main Track 3) - [Map](#)

Description:

What if a globally accessible maritime communications network was co-opted for other than intended use? Our research tool demonstrates how defenders and users of AIS (the Automatic Identification System) might create and detect a covert communications channel that operates without a conventional server or internet connection.

DC10's Stealth Data Transport (Khan) [<https://share.google/Y5mFWV13VamaskHvq>] AIS Spoofing: A Tutorial for Researchers Dr. Gary Kessler [<https://share.google/ye0yai283P4mbq3Sj>] DC27's Hack the Sea (Julian Blanco) [<https://share.google/H7ExvRhCfSv32OEio>] DC33's Pirates of the North Sea (Bjørkhaug) [<https://share.google/97Y51J8DEbis1TTAd>] DC33's Navigating the invisible (Mehmet Onder Key & Furkan Aydogan) [<https://share.google/5jvqgyAgdLm18f7kR>] Amro, A., & Gkioulos, V. (2022, September). From Click To Sink: Utilizing AIS for Command and Control in Maritime Cyber Attacks. 27th European Symposium on Research in Computer Security (ESORICS) 2022, Copenhagen, Denmark, pp. 535-553. Lecture Notes in Computer Science (LNCS), 13556. DOI: 10.1007/978-3-031-17143-7_26

Speakers: T. Gwyddon "data" Owen, amp

SpeakerBio: T. Gwyddon "data" Owen

data is a retired Air Force Cyber Warfare Officer with over 20 years of operational experience. While no longer a fed, he's a CNODP and RIOT grad with a Comp Sci BS from the USAF Academy and a Master's in Cyber Ops from the Air Force Institute of Technology. He's been certified in all 3 NSA Red Team work roles, all 3 offensive SIGINT work roles, qualified in all 6 Cybercom offensive work roles and personally engaged real-world, nation-state-level actors, malware and targets in air, land, sea, space & cyberspace both offensively and defensively. And he's done so with the US, UK, Canada, Australia and New Zealand. He also helped Bryce make the Space Badge for DEF CON 33 and the Clip-Boy badge for DEF CON 34.

SpeakerBio: amp

amp spent 10 years driving ships around the globe—now captains a CTF team instead. With a B.S. in electrical engineering and pursuing M.S. in info systems engineering, amp made the jump from maritime grit to digital ops, bringing salty sea stories and a screwdriver to every hacking challenge. They've co-hosted episodes of several podcasts poking at the strange edges of maritime security, cyber policy, and why everything breaks at 2 AM. Into hardware hacking, retro gaming, and running text-based RPGs where everything is a side quest.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Taming the Swarm: Hard Architectural Lessons from Building a Deterministic Agentic Web Pentesting System

Tags: DEF CON Official Talk | Demo

When: Saturday, Aug 8, 16:30 - 17:30 PDT

Where: LVCCW Level 1 Hall 3 904 (Main Track 4) - [Map](#)

Description:

Most agentic systems for offensive security boast impressive benchmarks while hiding the real cost, the real time, and the architectural pain behind them. Many remain closed-source, sacrificing the transparency security demands. After 20 years as an offensive security researcher, I spent the last 10 months distilling all that accumulated experience into a deterministic agentic pipeline for web pentesting. I'll dissect the hard trade-offs I had to make: why visual validation via Playwright, CDP and Vision models became mandatory (and why text-based parsing is architecturally broken for client-side vulns like XSS), why suppressing creativity backfired, how specialization, model shifting and temperature control enabled useful determinism, why a dedicated Skeptic agent and weighted scoring were essential, and why immutable audit trails, wet/dry separation and native MCP support became non-negotiable. War stories included: the "Dojo Incident" — where the agents decided rewriting server configs was cheaper than writing the exploit. Conclusion: reliable offensive agentic systems must be open-source. Closed-source hides real behavior and real risks. Open-source is not a license choice — it is the only architectural and ethical safeguard we have left.

SpeakerBio: Albert "yz9yt" Corzo

I've been breaking things for over 20 years — legally, most of the time. An offensive security researcher with an adversarial mindset, multiple Hall of Fame recognitions, and several critical CVEs discovered. For the past 6+ years I've focused on the intersection of AI and offensive security. My work centers on solving complex engineering challenges in agentic systems: enforcing determinism, minimizing token burn and environmental impact, and creating reliable pipelines that combine LLMs with real web pentesting tools. I'm a web pentester and technical speaker passionate about helping the next generation of researchers execute more precise and effective web attacks.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Blue Team Village - Friday - 13:15-14:15 PDT

Title: TBA

Tags: Blue Team Village | Creator Talk/Panel

When: Friday, Aug 7, 13:15 - 14:15 PDT

Where: LVCCW Level 2 W217 (Blue Team Village) Main Stage - [Map](#)

Description:

TBA



[Return to Index](#) - Add to Google

- ics [Calendar](#) file

Noob Community - Sunday - 10:00-13:59 PDT

Title: TCM Security Labs

Tags: Noob Community | Creator Event/Activity

When: Sunday, Aug 9, 10:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 4 1417 (Noob Community) - [Map](#)

Description:

TCM Security offers 250+ hours of practical, hands-on cybersecurity training across 28 courses and 13 certifications, built by hackers and trusted by teams. Drop in during village hours to work through their hands-on labs.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Noob Community - Friday - 10:00-17:59 PDT

Title: TCM Security Labs

Tags: Noob Community | Creator Event/Activity

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 4 1417 (Noob Community) - [Map](#)

Description:

TCM Security offers 250+ hours of practical, hands-on cybersecurity training across 28 courses and 13 certifications, built by hackers and trusted by teams. Drop in during village hours to work through their hands-on labs.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Noob Community - Saturday - 10:00-17:59 PDT

Title: TCM Security Labs

Tags: Noob Community | Creator Event/Activity

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 4 1417 (Noob Community) - [Map](#)

Description:

TCM Security offers 250+ hours of practical, hands-on cybersecurity training across 28 courses and 13 certifications, built by hackers and trusted by teams. Drop in during village hours to work through their hands-on labs.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Tech Reclaimers Update: A Year In, Building a Social Movement Away from Big Tech

Tags: Hackers.town | Creator Talk/Panel

When: Friday, Aug 7, 11:00 - 11:30 PDT

Where: LVCCW Level 1 Hall 3 1100 (Creator Stage 7) - [Map](#)

Description:

It has been a year since we launched the Tech Reclaimers, a social movement to help people reclaim their lives and their systems from Big Tech. And how far we have come! The community has grown online, with a thousand followers and hundreds of active participants in group chats. In this talk, describe our activities over the past year and our plans for the future, as well as what we have learned about the challenges people face in disentangling from Big Tech. While the technical challenges can be complicated, there are considerable social challenges too. And while hackers may look for the purest and best alternative options, we have found variety in meeting people where they are at to help them assemble the alternative stack that suits their needs, budget, skills, and values. Finally, we do indeed have friends everywhere: from the Rebel Tech Alliance to the Luddite Club, we discuss the connections we are forging and the new paths we are innovating.

Speakers: Andy Hull, Janet Vertesi, Rebecah Miller

SpeakerBio: Andy Hull, Officer at Tech reclaimers

No BIO available

SpeakerBio: Janet Vertesi, Officer at Tech Reclaimers

No BIO available

SpeakerBio: Rebecah Miller, Officer at Tech Reclaimers

No BIO available

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: TEE.fail: Breaking Trusted Execution Environments via DDR5 Memory Bus Interposition

Tags: DEF CON Official Talk | Demo | Exploit

When: Saturday, Aug 8, 17:30 - 17:59 PDT

Where: LVCCW Level 1 Hall 3 1007 (Main Track 2) - [Map](#)

Description:

Trusted execution environments (TEEs) aim to offer strong privacy and integrity guarantees even in the presence of root level attackers. Recently there has been a pivotal shift in TEE deployment, moving TEEs from enclaves running on PC-oriented hardware to confidential virtual machines executing on server-grade CPUs. Under the hood, this change has also resulted in significant modifications to the underlying memory encryption engine, removing integrity guarantees as well as protections against replay attacks. While Intel's and AMD's change in TEE implementation is clearly significant and substantial, most TEE deployments appear to fail to acknowledge the difference in security guarantees, assuming a stronger security model than truly afforded by the implementation. Thus, in this talk we discuss the true protection offered by Intel's and AMD's newest TEE offerings against entry-level physical side-channel attacks. We show that bus interposition attacks on DDR server memory can be constructed cheaply by hobbyists, using parts on e-commerce websites. With our bus interposer combined with the weaker security model of server TEEs, we will show a live demo of our ability to extract secret key material from machines in fully trusted status. Finally, we demonstrate the implications of our attacks on real world deployments.

<https://tee.fail> Paper: <https://tee.fail/files/paper.pdf> Please see our paper for references to prior work.

Speakers: Daniel Genkin, Jalen Chuang

SpeakerBio: Daniel Genkin, Georgia Tech

Daniel Genkin is an Associate Professor at the School of Cybersecurity and Privacy at Georgia Tech. Daniel's research interests are in hardware and system security, with particular focus on side channel attacks and defenses. Daniel's work has been recognized by best paper awards in multiple academic and industry venues, multiple Black Hat Pwnie awards, as well as covered by national and scientific press. Daniel has been part of the team performing the first analysis of speculative and transient execution, resulting in the discovery of Spectre, Meltdown and follow ups. Finally, he has a PhD in Computer Science from the Technion Israel's Institute of Technology and is a 2024 Alfred P. Sloan Research Fellow.

SpeakerBio: Jalen Chuang, Georgia Tech

Jalen Chuang is a PhD student at the Hardware Security Lab at Georgia Tech. Jalen's research spans software fuzzing, CPU microarchitectural side-channels, and now focuses on trusted execution environments. Outside of research, Jalen is a regular CTF player and 2-time DEFCON CTF finalist.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Contests - Sunday - 10:00-11:59 PDT

Title: TeleChallenge

Tags: TeleChallenge | Contest

When: Sunday, Aug 9, 10:00 - 11:59 PDT

Where: LVCCW Level 1 Hall 1 107 (TeleChallenge) - [Map](#)

Description:

The TeleChallenge isn't just a puzzle challenge, it's an experience. We are super excited to show the plan for the tenth year in a row. Don't copy that floppy, but instead prepare to be immersed in an entirely new world where all of your hacker skills will be challenged (along with your 0xEA60 skills). This is a very tough contest to win, and is among the most challenging at DEF CON. Are you ready? Your first step is to find us, because part of the puzzle is discovering the puzzle.

Participant Prerequisites

You'll need a phone, your creativity and some hacker friends. It also helps to have access to a computer. Use the TeleChallenge as an excuse to meet people and form a team.

Pre-Qualification

We may have team registration in advance, but there is no pre-qualifier.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Contests - Saturday - 10:00-17:59 PDT

Title: TeleChallenge

Tags: TeleChallenge | Contest

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 107 (TeleChallenge) - [Map](#)

Description:

The TeleChallenge isn't just a puzzle challenge, it's an experience. We are super excited to show the plan for the tenth year in a row. Don't copy that floppy, but instead prepare to be immersed in an entirely new world where all of your hacker skills will be challenged (along with your 0xEA60 skills). This is a very tough contest to win, and is among the most challenging at DEF CON. Are you ready? Your first step is to find us, because part of the puzzle is discovering the puzzle.

Participant Prerequisites

You'll need a phone, your creativity and some hacker friends. It also helps to have access to a computer. Use the TeleChallenge as an excuse to meet people and form a team.

Pre-Qualification

We may have team registration in advance, but there is no pre-qualifier.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Contests - Friday - 10:00-17:59 PDT

Title: TeleChallenge

Tags: TeleChallenge | Contest

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 107 (TeleChallenge) - [Map](#)

Description:

The TeleChallenge isn't just a puzzle challenge, it's an experience. We are super excited to show the plan for the tenth year in a row. Don't copy that floppy, but instead prepare to be immersed in an entirely new world where all of your hacker skills will be challenged (along with your 0xEA60 skills). This is a very tough contest to win, and is among the most challenging at DEF CON. Are you ready? Your first step is to find us, because part of the puzzle is discovering the puzzle.

Participant Prerequisites

You'll need a phone, your creativity and some hacker friends. It also helps to have access to a computer. Use the TeleChallenge as an excuse to meet people and form a team.

Pre-Qualification

We may have team registration in advance, but there is no pre-qualifier.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Telecom Village - Sunday - 14:00-14:15 PDT

Title: Telecom Village CTF Awards Ceremony

Tags: Telecom Village | Creator Event/Activity

When: Sunday, Aug 9, 14:00 - 14:15 PDT

Where: LVCCW Level 3 W321 (Telecom Village) - [Map](#)

Description:



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Telecom Village - Saturday - 16:45-16:59 PDT

Title: Telecom Village CTF Closure

Tags: Telecom Village | Creator Event/Activity

When: Saturday, Aug 8, 16:45 - 16:59 PDT

Where: LVCCW Level 3 W321 (Telecom Village) - [Map](#)

Description:



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Telecom Village - Friday - 16:30-16:59 PDT

Title: Telecom Village CTF Closure

Tags: Telecom Village | Creator Event/Activity

When: Friday, Aug 7, 16:30 - 16:59 PDT

Where: LVCCW Level 3 W321 (Telecom Village) - [Map](#)

Description:



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Telecom Village - Sunday - 10:20-13:59 PDT

Title: Telecom Village CTF

Tags: Telecom Village | Creator Event/Activity

When: Sunday, Aug 9, 10:20 - 13:59 PDT

Where: LVCCW Level 3 W321 (Telecom Village) - [Map](#)

Description:

SpeakerBio: T-Mobile CTF Team

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Telecom Village - Friday - 10:00-10:20 PDT

Title: Telecom Village Inauguration

Tags: Telecom Village | Creator Talk/Panel

When: Friday, Aug 7, 10:00 - 10:20 PDT

Where: LVCCW Level 3 W321 (Telecom Village) - [Map](#)

Description:

SpeakerBio: Pankaj Sontakke

No BIO available



[Return to Index](#) - Add to Google

- ics [Calendar](#) file

Telecom Village - Friday - 17:00-17:59 PDT

Title: Telecom Village Open Forum: Talks & Workshops: Review, Highlights, and Key Learnings

Tags: Telecom Village | Creator Event/Activity

When: Friday, Aug 7, 17:00 - 17:59 PDT

Where: LVCCW Level 3 W321 (Telecom Village) - [Map](#)

Description:



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Telecom Village - Saturday - 17:00-17:59 PDT

Title: Telecom Village Open Forum: Talks & Workshops: Review, Highlights, and Key Learnings

Tags: Telecom Village | Creator Event/Activity

When: Saturday, Aug 8, 17:00 - 17:59 PDT

Where: LVCCW Level 3 W321 (Telecom Village) - [Map](#)

Description:



[Return to Index](#) - Add to Google - ics [Calendar](#) file

The Diana Initiative - Friday - 13:10-13:20 PDT

Title: Telecom Village Tour

Tags: The Diana Initiative | Creator Tour

When: Friday, Aug 7, 13:10 - 13:20 PDT

Where: LVCCW Level 1 South Lobby / Atrium - [Map](#)

Description:

Interested in visiting Telecom Village but afraid to go by yourself? The Diana Initiative is hosting tours! Follow a volunteer to Telecom Village and be introduced to the community and activities inside!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Bug Bounty Village - Saturday - 10:30-10:59 PDT

Title: Testing API Business Logic With AI Agents: What We Got Wrong First

Tags: Bug Bounty Village | Creator Talk/Panel

When: Saturday, Aug 8, 10:30 - 10:59 PDT

Where: LVCCW Level 1 Hall 3 1102 (Creator Stage 6) - [Map](#)

Description:

Automating API security testing sounds straightforward until you try it on an enterprise API with complex auth and business flows. Over the past year, we've been building AI agents to test business logic vulns. This talk is an honest account of what we got wrong in that process. We'll cover 3 specific failures: testing before we understood resource relationships (and what that did to our IDOR detection), over-relying on agents for things deterministic methods handle better, and ignoring domain context until it became impossible to ignore. Each failure changed how we built the system. Some of the lessons were obvious in retrospect. The goal is to give anyone working on similar problems an honest look at where automated business logic testing actually breaks down and why the gap between a clean test env and an enterprise API might be harder to close than it looks. Participants will understand why business logic flaws are different and how to use agentic architecture to detect them.

SpeakerBio: Samantha Pearlstein, Founding Solutions Engineer at Escape

Samantha is a solutions engineer with a strong background in security research, executive cyber resilience, and nation-state threats. As a former consultant at Accenture, she led cyber resilience initiatives for Fortune 100 executives, developed GenAI-powered security tools, and delivered workshops on emerging cyber challenges. Today, as a Sales Engineer at Escape, Samantha helps AppSec teams secure their APIs and SPAs, combining her passion for cybersecurity with hands-on problem-solving.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Texas Incidents - How we broke the OMAP-L138 Trusted Execution Environment

Tags: DEF CON Official Talk | Demo

When: Friday, Aug 7, 10:00 - 10:59 PDT

Where: LVCCW Level 1 Hall 3 906 (Main Track 3) - [Map](#)

Description:

In this talk, we'll discuss how we achieved the black-box compromise of the Trusted Execution Environment (TEE) of the Texas Instruments OMAP-L138, a popular SoC encountered in various PMR radios, satcom equipment and other embedded applications. These radios are frequently used in safety-critical roles, where integrity and service availability is paramount.

Through a painstaking iterative process, which includes building both a disassembler and a decompiler for the (hellish) DSP architecture, and through blind exploitation of the Texas Instruments ROM code underpinning the TEE functionality, we managed to abuse a (novel type of) timing side channel that exists when attempting to load (bogus) cryptographic modules into the TEE, allowing us to recover the manufacturer key within a minute.

The talk dives deep into the technical aspects of the attack, providing a rare perspective on how the simple primitive of "decryption isn't constant time" can ultimately be leveraged into a very tangible result: recovery of the device's full 128-bit AES key. Additionally, we discuss several ROM-based vulnerabilities, including one that enables full secure-mode code execution on the SoC.

Vulns are in ROM, so if you're so inclined: feel free to have fun with those on other OMAP-L138-powered devices.

Speakers: Carlo Meijer, Wouter Bokslag

SpeakerBio: Carlo Meijer, Midnight Blue

Carlo Meijer is a founding partner of the boutique security consultancy firm Midnight Blue and is most known for his research into TETRA, the MIFARE Classic Crypto1 RFID cipher, and the security of self-encrypting drives. Furthermore, Carlo regularly competes in the famous Pwn2Own hacking competition, where he is part of team PHP Hooligans.

SpeakerBio: Wouter Bokslag, Midnight Blue

Wouter Bokslag is a co-founding partner and security researcher at Midnight Blue. He is known for the reverse-engineering and cryptanalysis of several proprietary in-vehicle immobilizer authentication ciphers used by major automotive manufacturers as well as co-developing the world's fastest public attack against the Hitag2 cipher. He holds a Master's Degree in Computer Science & Engineering from Eindhoven University of Technology (TU/e) and designed and assisted in teaching hands-on offensive security classes for graduate students at the Dutch Kerckhoffs Institute for several years.

Recently heavily involved in the TETRA:BURST research and associated follow-up research, such as the recent reverse-engineering and analysis of the elusive TETRA End-to-End protocol. Also, a contributor of open-source SDR code.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: That's Not Your Agent: Why Zero Trust Can't Tell

Tags: AI Village | Creator Talk/Panel

When: Saturday, Aug 8, 14:30 - 14:59 PDT

Where: LVCCW Level 1 Hall 3 801 (Creator Stage 2) - [Map](#)

Description:

What happens when every request is authenticated, every permission is scoped, every action logged, and the breach still happens without a single alert? Zero Trust has been widely adopted to secure environments through continuous authentication and verification. But unlike human users, agentic AI is non-deterministic and autonomous by nature. The same agent, given the same task, will reason and act differently every time. It operates beyond the moment trust was granted, making decisions no human approved. Zero Trust has no reliable way to distinguish a legitimate agent from a compromised one. This talk examines why standard controls break down. Behavioural baselining cannot establish a deviation threshold for a system with no stable baseline. IAM scoping cannot contain a compromised agent operating entirely within its authorised permissions. Continuous verification rechecks identity, not intent. When compromise occurs at the semantic layer, after authentication has already passed, every control evaluates correctly and finds nothing wrong. We map real-world disclosed incidents onto the attack vectors of a typical agentic architecture, identifying precisely where each Zero Trust control fails during the agent lifecycle. We then demonstrate a live compromise inside a correctly configured Zero Trust environment, showing two simultaneous views: what the defender sees in the logs, and what is actually happening. An indirect prompt injection attack, delivered through a poisoned document, rewrites the agent's instructions from inside its own context window. Data exfiltration follows through authorised API calls. Zero violations fire. The logs show a clean run. The data is already gone. We close with concrete mitigations from CSA's Agentic Trust Framework and MCP security guidance that teams can begin applying today. Zero Trust controls who started the session. It has no visibility into who is running it now.

Speakers: Krity Kharbanda, Emma Yuan Fang

SpeakerBio: Krity Kharbanda

Krity Kharbanda is a Senior Application Security Engineer at ServiceNow, focused on application security, cloud security, and emerging AI-driven attack surfaces. Alongside her technical work, she leads community and professional development initiatives at Breaking Barriers Women in Cybersecurity (BBWIC), fostering mentorship, growth, and collaboration across the cybersecurity community. A frequent conference speaker, she is passionate about translating deep technical security research into practical insights while creating meaningful impact through community engagement.

SpeakerBio: Emma Yuan Fang

Emma is a seasoned Security Architect specialising in cloud security and AppSec. As Regional Practice Lead at EPAM, she leads a team of security practitioners across the UK&I, Switzerland, and Germany. Her focus has recently expanded into the intersection of LLMs, MCP, and security, exploring how agentic AI systems reshape the threat landscape. Beyond her day job, Emma is an award-winning conference speaker, a dedicated mentor, and Vice President of WiCyS UK&I, where she champions diversity in the cyber workforce.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Cloud Village - Saturday - 16:00-16:40 PDT

Title: The 100-to-1 Problem: Securing the Non-Human Identity Perimeter

Tags: Cloud Village | Creator Talk/Panel

When: Saturday, Aug 8, 16:00 - 16:40 PDT

Where: LVCCW Level 3 W313 (Cloud Village Talks) - [Map](#)

Description:



[Return to Index](#) - Add to Google - ics [Calendar](#) file

DEF CON Talks - Friday - 11:00-11:59 PDT

Title: The 2026 Pwnie Awards

Tags: DEF CON Official Talk | The Pwnie Awards

When: Friday, Aug 7, 11:00 - 11:59 PDT

Where: LVCCW Level 1 Hall 3 1006 (Main Track 1) - [Map](#)

Description:

Speakers: Ian Roos, Mark Trumbour

SpeakerBio: Ian Roos

No BIO available

SpeakerBio: Mark Trumbour

No BIO available

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Malware Village - Friday - 14:10-17:25 PDT

Title: The Achaean project-Trojan development for noobs

Tags: Malware Village | Creator Workshop

When: Friday, Aug 7, 14:10 - 17:25 PDT

Where: LVCCW Level 1 Hall 2 600 (Malware Village) Workshops - [Map](#)

Description:

4 hour workshop. 1hr Lecture on trojan creation. Followed by 2 hrs hands on practice creating trojans, setting up malware servers. Using C## loaders and malicious dll's to trojanise normal programs with ransomware. Instructor aide and easy to follow instructions throughout.

1 hr CTF. Students will develop their own new trojan containerize it and send to our victim computer. Prizes.

SpeakerBio: Leigh Gilbert, Malware village

Leigh Trinity is a Canadian exploit developer, red team hacker, and instructor known for her work in binary exploitation and reverse engineering. Now branching out into malware development.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: The Agent Asked. We Allowed. Now What?

Tags: AppSec Village | Creator Event/Activity || All Audiences

When: Sunday, Aug 9, 12:45 - 13:45 PDT

Where: LVCCW Level 1 Hall 2 604 (Appsec Village) Arsenal - [Map](#)

Description:

AI agents are already running on developer machines, inside terminals, IDEs, and internal workflows. They are useful, but they can also read code, access files, execute commands, call tools, use credentials, and send data to LLM providers.

In this Arsenal demo, we will present an open-source runtime discovery tool for identifying LLM-powered applications and AI agents on live machines without requiring code changes. The tool correlates local processes with LLM-provider traffic, detects known and unknown AI service usage, monitors subprocess and file activity, and applies basic policy controls for coding agents.

We will show what AI agents look like at runtime, what they do beyond the chat interface, and how AppSec teams can see, understand, and control them.

Speakers: Liran Lavi, Sarit Yerushalmi

SpeakerBio: Liran Lavi

A senior security researcher from Tel Aviv specializing in web application security and advanced bot detection. With over 9 years of experience with small and large companies. To balance my tech-savvy life, you might find me hiking or skydiving - chasing new heights both literally and technically. I am always exploring edge cases and smarter ways to build and break systems.

SpeakerBio: Sarit Yerushalmi

Sarit Yerushalmi is an experienced security researcher at Imperva. Her research mainly focuses on application security and APIs. She analyzes traffic to detect new threats, writes security blogs and talks at conferences. Some of her work has been presented at security conferences such as Botconf, Bsides TLV, NorthSec, and Kernelcon.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: The Agent Long Con: Tricking Agents Out of Their Data

Tags: Crypto & Privacy Village | Creator Talk/Panel

When: Saturday, Aug 8, 15:00 - 15:59 PDT

Where: LVCCW Level 1 Hall 3 1103 (Creator Stage 5) - [Map](#)

Description:

Continuously running AI agents like OpenClaw are everywhere now and they're connected to everything. And despite all the doomposting, they're mostly unhacked. So what gives? Why isn't there a hacker gold rush against these systems?

In this talk, we break down why the classic prompt injection playbook is failing against modern agent systems including OpenClaw. A single malicious webpage or email is not enough to hijack an agent in 2026. We'll cover what's changed to make that true.

We'll demonstrate attacks showing the ones that fizzle out and the ones that land in order to highlight which defenses are working and which ones are falling apart.

Finally, we'll shift from smash-and-grab exploits to something far more effective: the long con. By chaining subtle manipulations over time, we'll show how attackers can steer, poison, and ultimately subvert AI agents for fun and profit.

SpeakerBio: Patrick Walsh

Patrick Walsh has an over 20 year history of running threat research and engineering teams overseeing products ranging from anti-virus and intrusion prevention to enterprise cloud software. He is a long-time advocate for privacy and security and holds multiple patents in that space. More recently, Patrick has built solutions to protect AI data and workflows. Patrick now leads IronCore Labs, an application data protection platform that uses encryption to protect data stored in the cloud while keeping it searchable and usable. Outside of work, he enjoys the outdoors, photography, hacking, lock picking, biking, swimming, and magic.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: The Agentic Free Pass: Does an Abliterated Backbone Make Agents Easier to Attack?

Tags: AI Village | Creator Talk/Panel

When: Saturday, Aug 8, 14:00 - 14:59 PDT

Where: LVCCW Level 1 Hall 2 603 (AI Village) - [Map](#)

Description:

This is a sit down discussion in a more casual conversational format: Attacking an AI agent? The reflex is to reach for an abilitated model, an LLM with the refusal direction surgically removed, on the assumption that stripping safety makes a stronger attacker. Open-source pentest frameworks run on them by default. We tested base and abilitated Qwen3 and Gemma-3 across agentic attack classes. It depends on the attack.

For soft agentic-artifact attacks, writing a poisoned RAG document, a malicious agent skill, an MCP tool-poisoning description, even aligned base models comply almost universally; the agentic frame alone is enough. The sharpest case: wrapping a harmful request as a tool call drops base Qwen3 from 98% to 44% safe, with no weights changed. We demo it live, one line of agent scaffolding undoing alignment that took billions of parameters. Goal hijacking succeeds about 92% regardless of model.

But when the agent needs genuinely hard content, malware and exploit code, weapons, illicit drugs, the backbone suddenly matters: abilitation roughly doubles success (Gemma 25% to 77.5%, Qwen 37.5% to 60%), and abilitated Gemma-3 is far more dangerous than abilitated Qwen3.

That divergence doubles as a detector. We release a defender test suite: a success rate above 50% on the hard categories is a strong sign the model in your stack has been abilitated.

Which abilitated model you pick barely changes easy agentic attacks but strongly changes hard ones. Per-layer probing predicts which abilitate cleanly. We release the harness, probe set, and detector.

Speakers:Karol Piekarski,Nishith Sinha

SpeakerBio: Karol Piekarski, DevOps Engineer

Karol Piekarski is a Lead DevOps Engineer working across cloud infrastructure, zero-trust architecture, and AI and agentic security for systems that serve hundreds of millions of consumers. His research focuses on the security of large language models and autonomous agents, with an emphasis on practical red-teaming and defensive tooling that teams can actually operationalize rather than shelve.

His empirical work on abilitation and agentic framing reframes where alignment actually breaks down in agent pipelines: agentic framing alone can collapse a model's baseline safety, while abilitation matters mostly for the hardest content and is highly architecture-dependent. In 2026 he co-presented "Move Fast, Stay Secure: Enterprise AI Agent Security in Practice" at the Databricks Data + AI Summit, and spoke at ScaLE 23x on open source red-teaming for LLMs. He was one of only two external contributors to the Databricks Agentic AI Security Framework (DASF v3.0).

Karol is the creator of Sundew.sh, an open source, MCP-native AI agent honeypot platform that uses behavioral fingerprinting and a persona engine for anti-fingerprinting, now adopted by external research teams studying agent behavior in the wild. He was selected as a Wiz MVP last year and this year received Wiz's Thought Leader award, and he is active in the AISECA Working Group, where he co-owns agentic security risk definitions.

He holds the CCSP, CKA, four AWS specialty certifications along with DataDog and Tines, and he regularly judges and mentors at hackathons across Southern California.

SpeakerBio: Nishith Sinha

Nishith Sinha started his career by pulling secrets out of thin air. As a researcher at Georgia Tech, he co-authored a side-channel attack that recovered RSA private keys from OpenSSL by reading its electromagnetic emissions alone. No code executed, no system touched. Presented at USENIX, the work prompted a rapid fix from the OpenSSL team and is still cited as a landmark example of hardware-level cryptographic risk.

It set the tone for what came next: a career built on finding the security gaps other people aren't looking at. At Cisco, that meant network security, where he helped design the company's firewall migration tooling. At Amazon, it meant identity, where he owned IAM strategy across tens of thousands of AWS accounts, and then application and cloud security, remediating critical vulnerabilities at enterprise scale. As generative AI took hold, Nishith moved with it, leading application security for Amazon Bedrock and Amazon Q, before building security from scratch for Amazon's Nova foundation models, safeguarding training data, model artifacts, and infrastructure across hundreds of teams.

Today, Nishith brings that range to Databricks, where he leads AI Security and the company's work on Agentic Security, AI Red Teaming, and AI Enterprise Security. He holds 10 AI security patents spanning model artifact protection, secure execution of model-initiated computer actions, and behavioral-analytics-based content moderation. He co-authored the Databricks Agentic Security Framework (DASF) and is credited with several CVEs. His focus now is autonomous AI agents: the newest layer of the stack, and the one attackers understand least.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: The Agentic Free Pass: Does an Abliterated Backbone Make Agents Easier to Attack?

Tags: Middle Easterns & Africans in Cyber Security (MEACS) | Creator Talk/Panel

When: Friday, Aug 7, 14:00 - 14:59 PDT

Where: LVCCW Level 1 Hall 4 1306 (Middle Easterns & Africans in Cyber Security (MEACS) Community) - [Map](#)

Description:

To attack an AI agent, the reflex is an abliterated model - refusal behavior surgically removed, expecting a stronger attacker. We tested that across open-weight models (Qwen3, Llama-3.1, the 754B GLM-5.2), scoring only attacks that actually fire a tool, not ones that just describe one.

Abliteration does make a tireless attacker. Asked to write attack payloads — poisoned RAG docs, malicious tool descriptions, injections — an abliterated GLM-5.2 said yes roughly three times as often as its base (13% → 38%). Pointed at an aligned copy of itself, it jailbroke that copy 80% of the time on the first try, and lifted its hidden system prompt. Set loose in a real coding agent (OpenCode) attacking an aligned-model app, it found exploits on its own: faking a password-reset to send a phishing email, and a KYC passed result to skip an identity check and wire money.

But look at how it won: blunt jailbreaks (ignore your instructions, SYSTEM OVERRIDE) failed about 100 times. Every win came from disguise — reframing the harmful step so it looked routine. Aligned agents block harm they recognize and fall for harm they don't.

The backbone matters only for hard content — malware, weapons, drugs — where abliteration clearly raises success (Qwen3 37.5% → 60%, GLM-5.2 67.5% → 77.5%). And method matters: single-direction Heretic can't strip Llama-3.1's refusal, but eight-direction OBLITERATUS can. That gap is also a detector: a model that clears 50% on hard content, or eagerly writes attacks, is probably tampered.

Speakers: Karol Piekarski, Nishith Sinha

SpeakerBio: Karol Piekarski, DevOps Engineer

Karol Piekarski is a Lead DevOps Engineer working across cloud infrastructure, zero-trust architecture, and AI and agentic security for systems that serve hundreds of millions of consumers. His research focuses on the security of large language models and autonomous agents, with an emphasis on practical red-teaming and defensive tooling that teams can actually operationalize rather than shelve.

His empirical work on abliteration and agentic framing reframes where alignment actually breaks down in agent pipelines: agentic framing alone can collapse a model's baseline safety, while abliteration matters mostly for the hardest content and is highly architecture-dependent. In 2026 he co-presented "Move Fast, Stay Secure: Enterprise AI Agent Security in Practice" at the Databricks Data + AI Summit, and spoke at ScaLE 23x on open source red-teaming for LLMs. He was one of only two external contributors to the Databricks Agentic AI Security Framework (DASF v3.0).

Karol is the creator of Sundew.sh, an open source, MCP-native AI agent honeypot platform that uses behavioral fingerprinting and a persona engine for anti-fingerprinting, now adopted by external research teams studying agent behavior in the wild. He was selected as a Wiz MVP last year and this year received Wiz's Thought Leader award, and he is active in the AISECA Working Group, where he co-owns agentic security risk definitions.

He holds the CCSP, CKA, four AWS specialty certifications along with DataDog and Tines, and he regularly judges and mentors at hackathons across Southern California.

SpeakerBio: Nishith Sinha

Nishith Sinha started his career by pulling secrets out of thin air. As a researcher at Georgia Tech, he co-authored a side-channel attack that recovered RSA private keys from OpenSSL by reading its electromagnetic emissions alone. No code executed, no system touched. Presented at USENIX, the work prompted a rapid fix from the OpenSSL team and is still cited as a landmark example of hardware-level cryptographic risk.

It set the tone for what came next: a career built on finding the security gaps other people aren't looking at. At Cisco, that meant network security, where he helped design the company's firewall migration tooling. At Amazon, it meant identity, where he owned IAM strategy across tens of thousands of AWS accounts, and then application and cloud security, remediating critical vulnerabilities at enterprise scale. As generative AI took hold, Nishith moved with it, leading application security for Amazon Bedrock and Amazon Q, before building security from scratch for Amazon's Nova foundation models, safeguarding training data, model artifacts, and infrastructure across hundreds of teams.

Today, Nishith brings that range to Databricks, where he leads AI Security and the company's work on Agentic Security, AI Red Teaming, and AI Enterprise Security. He holds 10 AI security patents spanning model artifact protection, secure execution of model-initiated computer actions, and behavioral-analytics-based content moderation. He co-authored the Databricks Agentic Security Framework (DASF) and is credited with several CVEs. His focus now is autonomous AI agents: the newest layer of the stack, and the one attackers understand least.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Malware Village - Saturday - 16:15-16:55 PDT

Title: The AI Analysis Train is Leaving the Station: ALL ABOARD!!

Tags: Malware Village | Creator Talk/Panel

When: Saturday, Aug 8, 16:15 - 16:55 PDT

Where: LVCCW Level 1 Hall 2 600 (Malware Village) Talks - [Map](#)

Description:

It's 2026, and we are no longer waiting for the AI area to come of age. It's here! Are YOU adopting and adapting to AI-enabled workflows? If you don't, you'll simply be left behind. We can no longer sit back and say, "AI isn't there yet." Don't get me wrong: It's not "there," yet. But by the time AI is "there," you'll be well behind the pack in terms of knowing how to use it, what to expect from it, and more. Let's fix that! In this talk, we'll show you how to use AI for malware analysis via leveraging the new MCP server that has been integrated into REMnux. We'll be using a free distro, with free tools, with a free (well duh) MCP server. Point being: It's all free, it's all open/available, and it's here now. So get on board!

SpeakerBio: Ryan "@rj_chap" Chapman

Ryan Chapman is the author of SANS, FOR528: Ransomware and Cyber Extortion, course, teaches SANS, FOR610: Reverse Engineering Malware, course, and works as a threat hunter @ \$dayJob. Ryan has a passion for life-long learning, loves to teach people about ransomware-related attacks, and enjoys pulling apart malware. He has presented workshops at DEF CON and other conferences in the past and knows how to create a step-by-step instruction set to maximize hands-on learning.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: The Air Is Hostile: RF Trust Assumptions in Modern Security Systems

Tags: Red Team Village | Misc

When: Sunday, Aug 9, 12:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 1 309 (Red Team Village) Tactic Table 3 - [Map](#)

Description:

Modern security systems are no longer purely physical. Alarms, sensors, access control, cameras, locks, panic buttons, monitoring paths, and backup communications increasingly depend on wireless technologies such as Wi-Fi, BLE, Zigbee, LoRa, LTE, and cloud-managed IoT infrastructure. For red teams, this creates an important question: what happens when the environment these systems depend on becomes adversarial?

This talk reframes RF as a red team attack surface, not just a radio engineering problem. It explores how wireless dependencies create opportunities for reconnaissance, failure-mode discovery, protocol fingerprinting, operational disruption, vendor-claim validation, and physical security bypass modeling. Rather than focusing on illegal or unsafe demonstrations, the presentation emphasizes responsible adversary emulation: identifying RF trust assumptions, mapping wireless dependencies, and testing whether organizations understand how their security systems behave under degraded or hostile spectrum conditions.

Attendees will learn how red teams can incorporate RF into engagements without turning the work into tool-driven theater. The talk covers passive RF reconnaissance, wireless dependency mapping, signal availability assumptions, anti-jam marketing claims, fail-open/fail-secure behavior, alert fatigue, response workflows, and the gap between “detection” and actual resilience. It also shows how RF risks connect to broader red team objectives: access control evasion, alarm reliability, site resilience, executive protection, incident response readiness, and vendor due diligence.

SpeakerBio: Mitch Breton

Z3r0 is a senior offensive security and threat intelligence operator specializing in real-world adversary simulation, APT-focused threat analysis, and high-signal security assessments.

His work centers on helping organizations understand not just where they are vulnerable, but how real attackers would exploit those weaknesses and what to do next.

With a background spanning red team engagements, penetration testing, and intelligence-driven security research,

Z3r0 approaches every engagement from an adversary’s perspective. He focuses on identifying the small, often-overlooked control failures that enable outsized impact—privilege escalation paths, persistence mechanisms, trust boundary violations, and detection blind spots.

At NetPhantom Security, Z3r0 leads initiatives that blend threat intelligence, deception, and offensive testing to provide early warning and decision-grade insight. This includes building and operating intelligence pipelines, adversary profiles, and controlled deception environments that surface attacker behavior before it reaches production systems.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: The API Made Me Do It - Do Bad APIs Lead AI to Generate Vulnerable Code?

Tags: Intermediate | AppSec Village | Creator Talk/Panel

When: Saturday, Aug 8, 16:10 - 16:40 PDT

Where: LVCCW Level 1 Hall 2 604 (Appsec Village) Main Stage - [Map](#)

Description:

We blame the bot when AI-generated code is vulnerable, but what if it is just using the dangerous APIs we left on the table?

This talk tests whether API design can steer AI coding agents toward safer code. The same agent builds the same Java/Spring task app twice: once in a normal environment, and once in a constrained one with secure-by-default scaffolding, deny-by-default settings, safer abstractions, and bans on risky APIs.

The app includes authentication, authorization, task ownership, file upload, SSRF-prone link previews, and simulated paid features. The prompts describe product behavior, not security advice, so the comparison focuses on environment design rather than better prompting.

Both projects are analyzed with CodeQL and manual review to compare SAST findings, authorization flaws, unsafe file handling, SSRF risks, abstraction bypasses, and cases where wrappers hide risk instead of reducing it.

SpeakerBio: Yariv Tal

Yariv Tal is a senior developer, security researcher, and cofounder of Secure From Scratch, a venture dedicated to teaching developers secure coding from the very first line of code.

A summa cum laude graduate of the Technion, Yariv brings four decades of programming experience and years of university lecturing and bootcamp mentoring to the field of application security.

He lectures on secure coding in academia and the private sector, leads the OWASP-untrust project, and researches the intersection of AI and application security, with a focus on secure code generation, LLM evaluation, and secure-by-construction development.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: The Authentic Operator: Social Engineering Through Natural Delivery

Tags: Red Team Village | Misc

When: Saturday, Aug 8, 11:00 - 11:59 PDT

Where: LVCCW Level 1 Hall 1 309 (Red Team Village) Workshop Stage 2 - [Map](#)

Description:

Current social engineering training commonly teaches OSINT, pretexting, phishing, vishing, rapport building, elicitation, influence, framing, and nonverbal communication. That material is valuable, but much of it still treats the operator as interchangeable: learn the technique, pick the pretext, run the script. This workshop takes a different angle. The operator's natural communication style is part of the tradecraft. A social engineering approach fails when the operator cannot deliver it credibly under pressure.

The Authentic Operator teaches attendees to build social engineering approaches around their own personality, behavioral strengths, and natural delivery style. Some operators are credible as curious analysts. Others are stronger as frustrated customers, helpful insiders, nervous applicants, confident peers, or authority-adjacent professionals. Attendees will learn to identify which approach they can carry without overacting, then use that approach to support elicitation, rapport, and access-oriented objectives during authorized red team assessments.

The accompanying tactic is a hands-on operator-matching lab for 10–15 participants. Drawing from the author's own style, including turning an apparent lack of "brain-to-mouth filter" into a rapport-building advantage, attendees will examine how authentic self-disclosure, conversational momentum, humor, curiosity, or controlled oversharing can lower defenses and encourage reciprocity. Participants will complete a short operator-style self-assessment, receive fictional assessment objectives, select a natural delivery approach, and build an opening interaction designed to elicit information or move closer to access. The goal is not to teach people to "be anyone." The goal is to teach operators to use who they already are with discipline, realism, and ethical boundaries.

SpeakerBio: Joanna -

Joanna Wiggum is the founder and principal investigator of Countervail, a veteran-owned Washington State licensed private investigation agency focused on cyber-enabled fraud, impersonation, business email compromise, ransomware, and other digital loss matters. Her work centers on the trust, workflows, and dependency blindspots adversaries exploit to gain access, move money, and legitimize harmful action.

Before founding Countervail, Wiggum held cybersecurity leadership roles at Starbucks, Oracle, and Microsoft across red teaming, incident response, trust and safety, enterprise risk, and investigations. She built Starbucks' first red team, led Oracle's cloud red team and anti-abuse program, and directed investigations involving enterprise systems, air-gapped cloud environments, and emerging technologies at Microsoft.

Wiggum served 12 years in the United States Air Force in enlisted and commissioned roles spanning communications, operational planning, and bomber operations. Her military background includes support for U.S. Central Command air-to-ground communications tied to Operations Enduring Freedom and Iraqi Freedom, followed by mission planning and leadership in B-52 operations. She holds a Master of Human Relations and a Bachelor of Arts in International Security Studies from the University of Oklahoma.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: The Autonomous Insider

Tags: Cloud Village | Creator Event/Activity | Attack

When: Sunday, Aug 9, 11:00 - 12:59 PDT

Where: LVCCW Level 3 W311 (Cloud Village Labs) A - [Map](#)

Description:

In 2026, the 'Cloud Perimeter' has shifted from IP addresses to Agent Identities. This lab explores the intersection of Generative AI and Cloud Misconfiguration. We move beyond the prompt, demonstrating how classic architectural flaws-like over-permissive VPC Endpoints, missing IAM Conditions, and SSRF-prone Tool-call environments-allow attackers to turn a 'helpful' AI assistant into a cross-account exfiltration engine. Attendees will learn to exploit and then 'shackle' these agents using VPC Service Controls, SCPs, and automated remediation workflows.

Speakers:Naveen Reddy Pogalla,Hari Pranav Arun Kumar

SpeakerBio: Naveen Reddy Pogalla

Naveen works within the Product Security Engineering team at Google Cloud, operating at the intersection of data and defense. Specializing in Cloud Security Posture Management and engineering automated remediation accelerators, he analyzes the broader risk landscape to drive remediation and hardening at scale. Rather than just hunting for individual bugs, his goal is to build a more secure cloud by identifying and eliminating entire classes of vulnerabilities before they can be exploited. Naveen thrives on solving high-stakes security challenges that require a blend of analytical rigor and an offensive security mindset. Prior to Google, he empowered clients as a Security Consultant at EY and Grant Thornton, with expertise spanning network security, vulnerability assessments, and GRC. He holds a Master's degree in Cybersecurity Analytics and Operations from Penn State University and a Bachelor's in Computer Science Engineering.

SpeakerBio: Hari Pranav Arun Kumar

No BIO available

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: The Autonomous Security Loop

Tags: Cloud Village | Creator Event/Activity | Strategic Defense

When: Friday, Aug 7, 13:30 - 14:30 PDT

Where: LVCCW Level 3 W311 (Cloud Village Labs) B - [Map](#)

Description:

SOCs get thousands of alerts daily. Most orgs take days to triage and fix critical findings. Attackers exploit that gap.

This lab walks through the three stages of a continuous security loop. Do each phase by hand, then see how the latest AWS capabilities compress it to seconds:

Discovery: Review output from a continuous security scan that found a multi-step attack path. Understand why this catches things annual pen tests miss. Triage: Manually triage 5 out of 30 Security Hub findings using the same signals AI triage uses. Compare your calls against the automated system. Remediation: Examine proposed fixes. Understand the difference between human-approved and autonomous remediation. Submit a fix and confirm it works.

Speakers:Jeremy Schiefer, Lawton Pittenger

SpeakerBio: Jeremy Schiefer

Jeremy is a Pr. Security Solution Architect at AWS focused on helping customers improve their security posture.

SpeakerBio: Lawton Pittenger

Lawton is a Worldwide Security Specialist Solutions Architect at AWS, based in New York City. He specializes in helping customers design and implement effective network security controls. At AWS, he works with customers at scale and collaborates closely with service teams to drive continuous improvement in security services based on customer needs and feedback

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: The Autonomous SOC Blueprint: On-Premise ML & AI to Condense, Consolidate, Contextualize, Correlate & Co-Investigate Attack Chains Hiding in the Noise

Tags: Middle Easterns & Africans in Cyber Security (MEACS) | Creator Talk/Panel

When: Saturday, Aug 8, 17:30 - 17:59 PDT

Where: LVCCW Level 1 Hall 3 1100 (Creator Stage 7) - [Map](#)

Description:

In this talk, you'll learn to use on-prem auditable and tunable ML models to automatically: normalize events to any data model, enrich events with relevant labels across various frameworks and controls (eg: MITRE ATT&CK, NIST, CISA KEV, CCM, VERIS, CRI), group related events to shrink their volume and reveal coordinated activity, chain causal events to expose multi step attacks, and use AI with to generate and execute detailed context-rich incident investigations and response. Use ML to auto-enrich events with relevant ATT&CK TTPs, NIST 800-53, VERIS, CSA CCM, CISA KEV, CRI & controls in AWS, GCP, Azure, M365 and Intel vPro Use ML to auto condense, correlate, contextualize & connect events to expose attack chains hiding in the noise of false positives & isolated incidents Use private on-premise AI models with condensed, normalized, and correlated data to execute high-fidelity agentic workflows and investigations

SpeakerBio: Ezz Tahoun

Ezz Tahoun is an award-winning cybersecurity data scientist recognized globally for his innovations in applying AI to security operations.

He has keynoted, trained & presented at BlackHat US, Sector, MEA, Asia & EU, DEFCON, SANS Summits, all the top Bsides, Securityweek ICS Conference and GISEC among many others.

His groundbreaking work earned him a gold edison award and accolades from Yale, Princeton, Northwestern, NATO, Microsoft, and Canada's CSE.

At 19, Ezz began his PhD in Computer Sci at the Univ of Waterloo, quickly gaining recognition through over 20 influential papers and open-source tools.

His experience includes leading advanced AI security ops projects for Orange CyberDefense, Forescout, RBC, and Huawei US.

He holds certifications such as GIAC Advisory Board, aCCISO, CISM, CRISC, GCIH, CEH, PMP and GCP-Cloud Architect, and served as an adjunct professor in cyber defense and warfare.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Policy @ DEF CON - Saturday - 14:00-14:30 PDT

Title: The best of three bad ideas? Ransomware taxes in lieu of bans or doing nothing

Tags: Policy @ DEF CON | Creator Talk/Panel

When: Saturday, Aug 8, 14:00 - 14:30 PDT

Where: LVCCW Level 2 W210-211 (Policy Village) - [Map](#)

Description:

A common proposal to disrupt ransomware operations is to institute a ban on ransomware payments. That risks several unwanted effects including prolonged critical infrastructure outages, a feeling of revictimization, non-compliant payers being extorted over paying. This talk investigates the potential for a middle ground: A ransomware tax.

SpeakerBio: Joe Uchill

Joe Uchill is a PhD student in public policy at RAND Graduate School. Until recently, he was a reporter covering cybersecurity for outlets like Axios and The Hill.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: The Black PhD Playbook: What No One Tells You

Tags: Blacks In Cyber Village | Creator Talk/Panel

When: Friday, Aug 7, 11:00 - 11:55 PDT

Where: LVCCW Level 3 W322-W324 (BIC Village) - [Map](#)

Description:

Join us for an honest, encouraging, and relatable conversation about pursuing a PhD as a Black student or cybersecurity professional. Our panelists will share what the journey really looks like, including how they chose their programs, found research interests, secured funding, built support systems, handled self-doubt, and balanced school with the rest of life. Attendees will leave with practical advice, real-world lessons, and a better understanding of how to decide whether a PhD is the right path for them.

Speakers: Dr. Fatou Sankare, Dr. Xavier-Lewis Palmer, Dr. Tia Pope

SpeakerBio: Dr. Fatou Sankare, Cybersecurity Professional / Community Speaker

Dr. Fatou is a Cyber Engineer and an adjunct professor, dedicated to increasing cyber education, particularly in underestimated communities, through Dataction LLC, which they founded. They are a Certified Ethical Hacker and hold the AWS Machine Learning Specialty Certification.

SpeakerBio: Dr. Xavier-Lewis Palmer, Cybersecurity Professional / Community Speaker

Dr. Palmer is multi-disciplinary professional whose work focuses largely on biomedical contexts. He enjoys positive and creative projects that foster both curiosity and helpful conversations around technologies that interface with biology.

SpeakerBio: Dr. Tia Pope, North Carolina Agricultural and Technical State University

Dr. Tia Pope is a Principal at Base10 Partners, where she invests in machine intelligence and emerging AI technologies. She earned her PhD researching the evaluation and development of AI tools for protein design, with an emphasis on dual-use risks and cyberbiosecurity threats. Her work has included projects with MIT Lincoln Laboratory and Johnson & Johnson, bridging advanced research with real-world impact. Tia specializes in transformer-based models for protein engineering, function prediction, and biological risk assessment. She has also contributed to open-source efforts that expand access to cutting-edge bio-AI tools. Her work reflects a commitment to supporting secure, ethical, and resilient technologies at the intersection of machine learning, molecular design, cybersecurity, and venture investment.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: The Breach Is Over. The Exposure Is Not

Tags: Recon Village | Creator Talk/Panel

When: Saturday, Aug 8, 15:00 - 15:30 PDT

Where: LVCCW Level 1 Hall 3 801 (Creator Stage 2) - [Map](#)

Description:

Breaches are usually treated as discrete incidents. A leak is discovered, the most recognisable credentials are rotated, incident-response activity slows down, and attention moves to the next compromise. The exposure rarely ends with the incident. Credentials can remain valid for months, sometimes long enough to be reused in later attacks. While common credential types receive immediate attention, large breach datasets often contain hundreds of less familiar secret classes that are harder to recognise, validate, or prioritise. This talk examines the long tail of a major software supply chain breach and measures how exposed credentials age, which categories survive longest, and whether public disclosure actually results in remediation.

The leaked values are only part of the exposure. Secret names, environment variables, repository paths, service identifiers, deployment stages, and naming conventions can reveal how an organisation builds and operates its systems. Even when a credential has expired, this contextual residue can support attack-surface discovery, technology identification, infrastructure correlation, and future targeting. By looking beyond the obvious credential classes and focusing on the outliers, this talk demonstrates how breach data can be transformed into durable reconnaissance intelligence, and why recovery should be measured by the disappearance of usable exposure rather than the closure of the original incident.

Speakers: Kumar Ashwin, Anant Shrivastava

SpeakerBio: Kumar Ashwin, Security Researcher at RedHunt Labs

I work at the intersection of AI, blockchain, and software security — threat modeling complex systems, defining security strategies, and building tooling that scales secure-by-default practices across engineering teams. I work at RedHunt Labs, train at Black Hat, and have spoken at Black Hat, XeeFCon, nullcon, DEF CON, and other conferences worldwide.

SpeakerBio: Anant Shrivastava

Anant Shrivastava is the founder of Cyfinoid Research and a long time offensive security practitioner with a focus on application, cloud, and supply chain security. He has delivered trainings and talks at Black Hat (USA, Europe, Asia), Nullcon, c0c0n, BSides, Rootconf and multiple other events, and runs projects such as Hacking Archives of India to highlight real work from the security community. His courses are built from real consulting and red team experience, with an emphasis on attack chains that actually show up in the field and defenses that teams can implement the next day.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: The Call Stack Experience

Tags: AppSec Village | Creator Event/Activity || All Audiences

When: Saturday, Aug 8, 15:00 - 16:59 PDT

Where: LVCCW Level 1 Hall 2 604 (Appsec Village) POD 4 - [Map](#)

Description:

Let's play with blocks... and learn how real application attacks unfold.

You will build real application call stacks, one foam block at a time, with each block representing function calls in a normal execution flow.

Once your stack is complete, you will see first-hand how easy it is for exploits to blend in with normal application behavior.

SpeakerBio: Victoria Keeler

No BIO available

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: The Call Stack Experience

Tags: AppSec Village | Creator Event/Activity || All Audiences

When: Friday, Aug 7, 11:00 - 12:59 PDT

Where: LVCCW Level 1 Hall 2 604 (Appsec Village) POD 2 - [Map](#)

Description:

Let's play with blocks... and learn how real application attacks unfold.

You will build real application call stacks, one foam block at a time, with each block representing function calls in a normal execution flow.

Once your stack is complete, you will see first-hand how easy it is for exploits to blend in with normal application behavior.

SpeakerBio: Victoria Keeler

No BIO available

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: The Camera Is Lying: RTSP Trust Failures in Modern Surveillance Systems

Tags: IoT Village | Creator Talk/Panel

When: Saturday, Aug 8, 11:00 - 11:45 PDT

Where: LVCCW Level 1 Hall 3 1105 (Creator Stage 3) - [Map](#)

Description:

Surveillance cameras sit at the intersection of physical security, privacy, and critical infrastructure. Yet many still rely on decades-old streaming protocols and fragile trust assumptions that receive far less scrutiny than web interfaces or cloud APIs. In this talk, Bitdefender researchers present a newly discovered authentication bypass affecting Hikvision surveillance cameras that abuses RTSP session handling to gain unauthorized access to live video streams. By exploiting inconsistencies between session validation and authorization logic, attackers can transform low-privilege or permissionless sessions into authenticated stream access.

SpeakerBio: Bogdan "BOTEZATU"

No BIO available

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: The Closing Window: Governing Agentic AI Security in a Post-Mythos World

Tags: Policy @ DEF CON | Creator Talk/Panel

When: Saturday, Aug 8, 17:00 - 17:59 PDT

Where: LVCCW Level 2 W210-211 (Policy Village) - [Map](#)

Description:

Mythos changed the question. Agentic AI security tooling operating at production scale is no longer a research problem or a vendor concern, it is a governance emergency. The frameworks governments have built to manage cyber risk were not designed for systems that acquire credentials autonomously, execute decisions faster than any human authorisation loop, and integrate third-party components whose security provenance no procurement standard currently requires anyone to verify. This panel convenes policy practitioners from across the agentic AI security stack (cloud-native, endpoint, behavioural detection, and federal policy) to examine what governance must look like before agentic AI becomes irreversibly embedded across critical national infrastructure and government departments. Structured around five substantive policy topics with direct implications for US, UK, and EU regulatory frameworks, the session closes with concrete, jurisdictionally-grounded recommendations that government affairs professionals can act on, across CVE architecture, critical infrastructure designation, agent identity standards, incident reporting obligations, and procurement requirements, before the legislative windows currently open in all three jurisdictions close or retrofitting security becomes too costly.

Speakers: Taylor Roberts, Mitch Herckis, Katie Trimble-Noble, Razvan Gavrila

SpeakerBio: Taylor Roberts, Zenity

Taylor Roberts is a seasoned cyber and AI security policy expert with experience spanning academia, the US federal government, and the private sector, currently serving as Principal of AI Security Policy at Zenity. Previously the Global Director of Security and Trust Policy at Intel and a former Cybersecurity Advisor at the White House's Office of Management and Budget, Taylor works toward fostering collaboration with governments, industry, and standards organizations to strengthen the AI security cybersecurity ecosystem. He holds a Masters in International Affairs from UC San Diego.

SpeakerBio: Mitch Herckis, Wiz

Mitch Herckis has spent two decades working with and for the public sector on technology and security policy. Currently, Mitch serves as the Global Head of Government Affairs for Wiz, a cloud cybersecurity company. Prior to joining Wiz, Mitch served as Director of the Federal Cybersecurity Branch within the White House's Office of Management and Budget, where he led cybersecurity initiatives within the Office of the Federal Chief Information Officer, including implementation on the President's Executive Order on Improving the Nation's Cybersecurity. Before joining federal service, Mitch served as a Senior Advisor for New York City Cyber Command, facilitating security implementations across 100+ city agencies on behalf of the City's central cybersecurity authority. He also spearheaded public initiatives to increase the digital security of City residents. Mitch has advocated for sound technology policies at all levels of government, including serving as the Director of Government Affairs for the National Association of State Chief Information Officers (NASCIO), and Senior Legislative Counsel for Federal Relations at the National League of Cities.

SpeakerBio: Katie Trimble-Noble, Director, PSIRT and Bug Bounty

Katie serves as a CVE Program Board, Bug Bounty Community of Interest Founder, and Hacking Policy Council Founding member. She is a passionate defensive cybersecurity community activist, she is regularly involved in community driven projects and is most happy when she is able to effect positive progress in cyber defense. In her day job Katie Noble serves as a Director of PSIRT, specializing in Global Secretarial Policy and Industry Engagement and Bug Bounty, at a fortune 50 Technology Company. Prior to joining private sector, Katie spent over 15 years in the US Government. Most recently as the Section Chief of Vulnerability Management and Coordination at the Department of Homeland Security, Cyber and

Infrastructure Security Agency (CISA). Her team is credited with the coordination and public disclosure of 20,000+ cybersecurity vulnerabilities within a two-year period. During her government tenure, in roles spanning Intelligence Analyst for the National Intelligence Community to Senior Policy Advisor for White House led National Security Council Cyber programs, Katie’s work directly impacted decision making for government agencies in the United States, United Kingdom, Canada, and Australia.

SpeakerBio: Razvan Gavrilă, ENISA - The European Union Agency for Cybersecurity

Razvan Gavrilă is a seasoned cybersecurity professional with over 15 years of experience across national and EU institutions. In his current role, he oversees ENISA’s work on the implementation of the EU Cyber Resilience Act and leads initiatives in product and security engineering, including the cybersecurity of AI systems. Prior to his appointment as Head of Sector for Market, Technology, and Product Security in January 2025, he served as ENISA’s lead Cyber Threat Intelligence (CTI) analyst. He holds several industry-recognized certifications and a Master of Science in Computer and Information Security

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: The Compiler Nobody Satisfactorily Tested: Supply-Chain Gaps in EV Charging Firmware

Tags: Car Hacking Village | Creator Talk/Panel

When: Saturday, Aug 8, 15:30 - 15:59 PDT

Where: LVCCW Level 1 Hall 3 801 (Creator Stage 1) - [Map](#)

Description:

Someone installed Doom on an Alpitronic supercharger at Pwn2Own Automotive 2026 — via an out-of-bounds write in firmware compiled by a compiler nobody verified. This talk connects the dots between Pwn2Own exploit classes and the upstream problem: most automotive and EVSE compilers have never been independently tested against safety or security standards. I will present a map of which compilers are actually qualified, where the coverage gaps are, and why Rust's memory safety guarantees matter less than you think if the compiler itself isn't verified. The talk closes with a practical trust chain — develop, compile, verify, review — that the security community can use to evaluate toolchain integrity.

SpeakerBio: Kangwon Lee, Life Member of OWASP

In computing since '86 (HS computer club EMPAL BBS Yonsei). Radar application algorithms at Autoliv, embedded SW at Hyundai Motor. Now Associate Prof at TU Korea, interested in Rust compiler qualification for safety-critical ITS. IEEE ITSS Korea Chapter Chair, IEEE P3538 WG Secretary, OWASP lifetime member, ISC2 CC. Sits on Korea's government committee on motor vehicle safety defects. Ph.D. ME + M.S. EECS, U of Michigan.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: The Compiler That Can't Read: Crashing Every 5G Phone With One Byte

Tags: DEF CON Official Talk | Demo | Exploit

When: Saturday, Aug 8, 16:00 - 16:59 PDT

Where: LVCCW Level 1 Hall 3 903 (Main Track 5) - [Map](#)

Description:

Every 5G phone parses radio messages using code generated by a compiler. That compiler has two blind spots — and we used them to crash iPhones, Pixels, and phones from every major chipset vendor. No credentials, no user interaction, no warning.

The compiler can't read English. Hundreds of rules that govern when fields should appear exist only in natural-language prose. The compiler discards them all. We extracted these invisible rules, turned them into targeted payloads, and crashed basebands from Apple, Google, Qualcomm, and MediaTek — all before authentication. Apple confirmed reproduction. Google Android Security confirmed multiple findings. MediaTek patched three CVEs affecting 64 chipset models and over 542 smartphone models. Qualcomm rewarded one finding.

The compiler can't count. Some fields have value ranges that don't fill the wire encoding. We changed one byte in a legitimate message and crashed phones across two chipset generations. GSMA assigned CVD-2025-0110.

Same root cause, same blind compiler, same result: the modem trusts a decoder that was never built to enforce the rules that matter. We demo live over-the-air crashes on stage.

1. 3GPP TS 38.331: NR Radio Resource Control (RRC) protocol specification
2. 3GPP TS 33.501: Security architecture and procedures for 5G System
3. ITU-T X.680-X.693: ASN.1 and encoding rules (UPER)
4. Hernandez et al., "FirmWire: Transparent Dynamic Analysis for Cellular Baseband Firmware," NDSS 2022
5. Klischies et al., "BaseBridge: Bridging the Gap Between Over-the-Air and Emulation Testing for Cellular Baseband Firmware," IEEE S&P 2025
6. Garbelini et al., "5Ghoul: Unleashing Chaos on 5G Edge Devices," IEEE TDSC 2025
7. Park et al., "DoLTEst: In-depth Downlink Negative Testing Framework for LTE Devices," USENIX Security 2022
8. Rupprecht et al., "Putting LTE Security Functions to the Test: A Framework to Evaluate Implementation Correctness," USENIX WOOT 2016

Speakers: Qiqing Huang, Xingyu Wang

SpeakerBio: Qiqing Huang

Qiqing Huang is a PhD candidate in Computer Science at the University at Buffalo, specializing in 5G baseband security. His research focuses on exploiting structural gaps between formal protocol schemas and natural-language specification constraints to discover pre-authentication vulnerabilities in commercial cellular modems. His work has resulted in multiple high-severity CVEs affecting major baseband vendors including Apple, Qualcomm, Samsung, and MediaTek, impacting 64 chipset models and over 542 commercially available smartphone models. He received GSMA CVD-2025-0110 for discovering a class of ASN.1 decode divergence vulnerabilities. His research has been published at USENIX Security 2026. He maintains active responsible disclosure relationships with Apple, Google, Qualcomm, Samsung, MediaTek, and GSMA. He is completing his PhD in Summer 2026 and is on the job market for security research roles.

SpeakerBio: Xingyu Wang, University at Buffalo

Xingyu Wang is a PhD student at the University at Buffalo studying the weird edge cases of networks, phones, and systems that are supposed to "just work." He explores how AI can help security researchers survive dense specs and turn "wait, why

did it do that?” moments into better tests. He does not fully trust AI or complex systems, but he enjoys putting them in the same room and watching what breaks first.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Blacks In Cyber Village - Friday - 15:00-15:25 PDT

Title: The Cost of Unverified Intelligence: AI and Accountability in Defense Operations

Tags: Blacks In Cyber Village | Creator Talk/Panel

When: Friday, Aug 7, 15:00 - 15:25 PDT

Where: LVCCW Level 3 W322-W324 (BIC Village) - [Map](#)

Description:

Explore the critical implications of unverified intelligence in defense operations, particularly concerning the role of Artificial Intelligence. This presentation will delve into a recent incident where AI-processed data contributed to a devastating error, examining the failure points in human oversight, algorithmic accountability, and the growing workforce gap in understanding and managing these powerful systems. Join us to discuss the urgent need for robust governance, verification, and training infrastructure to ensure responsible AI deployment in defense, and consider what lessons must be learned to prevent future tragedies. This timely discussion draws on current doctrine, recent operations, and ongoing public discourse, offering valuable insights for anyone interested in AI ethics, national security, and responsible technology development.

SpeakerBio: Kayrene Woods, Graduate Student, Founding President of BiC ODU

Kayrene Woods is an emerging cybersecurity professional and recent graduate of Old Dominion University, where they earned a B.S. in Cybersecurity with a minor in Computer Science and a 3.76 GPA as a member of the Perry Honors College. Notably, they served as the Founding President of the Blacks in Cybersecurity ODU chapter, which is the second officially recognized chapter established outside of the parent organization. Their technical expertise and research spans cybersecurity engineering, network security, intrusion-detection, and AI governance, with hands-on experience from an internship at the Air Force Research Laboratory/Griffis Institute supporting Department of Defense security research. This summer, they'll serve as a VICEROY Envoy at the Pentagon, supporting a Cloud Portfolio project for Air Force Intelligence within the Chief Information Officer's unit.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: The Cum-Stained Precipice of Digital Redlining

Tags: Hackers.town | Creator Talk/Panel

When: Friday, Aug 7, 13:00 - 13:30 PDT

Where: LVCCW Level 1 Hall 3 1100 (Creator Stage 7) - [Map](#)

Description:

The web was supposed to democratize information. Instead, we have a two-tier reality: one class consuming porn on \$2,000 laptops they'll discard in eighteen months, another class without a screen. The web was supposed to democratize information. Instead, we have a two-tier reality: one class consuming porn on \$2,000 laptops they'll discard in eighteen months, another class without a screen. That discarded laptop could have been a classroom, a business, a lifeline. The gap between those two realities is a political choice—one we can make differently. This talk is a direct confrontation with the culture of disposable tech—and a practical guide to grassroots reclamation programs that turn waste into opportunity and combat inequality with community.

Speakers: Erica Rachel Andrews, Abbie Gonzalez (pronounced AB)

SpeakerBio: Erica Rachel Andrews, Co-founder and president at Springfield.community

No BIO available

SpeakerBio: Abbie Gonzalez (pronounced AB), Executive Director Springfield.community

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: The CVE-Hunters Project: From Noobs to Researchers

Tags: La Villa Community | Creator Talk/Panel

When: Saturday, Aug 8, 13:30 - 13:59 PDT

Where: LVCCW Level 1 Hall 4 1416 (La Villa Community) Main Stage - [Map](#)

Description:

What if publishing a CVE wasn't reserved for elite hackers, but achievable by anyone with the right mindset, method, and community?

This talk tells the story of how the Brazilian CVE-Hunters Project transformed beginners with zero published research into recognized vulnerability researchers contributing to global cybersecurity. By breaking down the myth that CVEs require genius-level exploits or zero-days, we reveal a structured, repeatable methodology that turns curiosity into impact.

You'll learn how vulnerability research can be systematized, how responsible disclosure really works behind the scenes, and how publishing your first CVE can change your technical credibility, career trajectory, and confidence.

More than a technical presentation, this is a blueprint for moving from learning hacking to becoming a researcher — and contributing meaningfully to the security ecosystem.

Because your first CVE isn't about ego.

It's about responsibility, growth, and raising the bar for global security.

SpeakerBio: Natan Morette, Pentest Manager at Thoropass, vulnerability researcher, and cybersecurity instructor for Brazil's national Hackers for Good initiative

Natan Morette is a Penetration Test Manager, vulnerability researcher, and cybersecurity instructor for Brazil's national Hackers for Good initiative, where he mentors students in offensive security across the country. He began his career as a help desk analyst and moved through infrastructure roles before discovering his passion for cybersecurity. Natan has discovered and published multiple CVEs and actively supports students in identifying and disclosing their own—especially in open-source projects with meaningful social impact.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: The Cyber Crystal Ball: The Annual Policy @ DEF CON Contingencies Survey

Tags: Policy @ DEF CON | Creator Talk/Panel

When: Friday, Aug 7, 13:00 - 13:59 PDT

Where: LVCCW Level 2 W210-211 (Policy Village) - [Map](#)

Description:

Starting at DEF CON 33 Policy @ DEF CON shared the results of experts predictions regarding a range of cyber contingencies. With a year under our belts we can take a look at how the experts did with their prognostication last year, and look forward towards potential outcomes in the coming year. We will compare answers from year to year, and we've added a few new questions along with expanding the roster of expert respondents. The panel discussion with experts will explore how the outcomes of cyber contingencies will affect geopolitics between now and DEF CON 35.

Speakers: Matthew Wein, Bruce Schneier, Chris Painter, Heather West

SpeakerBio: Matthew Wein, Policy @ DEF CON

Matthew is a national security policy expert with over 15 years of experience in the Executive and Legislative branches of government and the private sector. This is his second year producing the DEF CON Contingencies Survey.

SpeakerBio: Bruce Schneier, Advisory Board Member at VerifiedVoting.org

Bruce Schneier is an internationally renowned security technologist, called a “security guru” by the Economist. He is the New York Times best-selling author of 14 books – including *Rewiring Democracy* and *A Hacker’s Mind* -- as well as hundreds of articles, essays, and academic papers. His long-running newsletter and blog, “Schneier on Security,” is one of the most popular sources of cybersecurity news on the internet. Schneier is a Fellow and Lecturer in Public Policy at the Harvard Kennedy School and the Munk School at the University of Toronto. He is a fellow at the Berkman-Klein Center for Internet and Society at Harvard University, a board member of the Electronic Frontier Foundation and AccessNow, and an advisory board member of EPIC and VerifiedVoting.org. He is also the Chief of Security Architecture at Inrupt, Inc.

SpeakerBio: Chris Painter

Christopher Painter is a globally recognized leader on cyber policy, cyber diplomacy, cybersecurity and combatting cybercrime. He has been at the vanguard of cyber issues for over 30 years, first as a federal prosecutor handling some of the most high-profile cyber cases in the U.S., then as a senior official at the U.S. Department of Justice, the FBI, the White House National Security Council and, finally, as the world’s first cyber diplomat at the U.S. Department of State. Among many other things, Chris is currently a Founding Partner of The Cyber Policy Group.

SpeakerBio: Heather West, Eurasia Group

Heather West is a policy and tech translator, product consultant, and long-term digital strategist guiding the intersection of emerging technologies, culture, governments, and policy. Equipped with degrees in both computer and cognitive science, Heather focuses on data governance, data security, artificial intelligence (AI), and privacy in the digital age. She is a subject matter authority who has written extensively about AI and other data driven topics for over a decade. She is also a member of the Washington Post's The Network, a group of high-level digital security experts selected to weigh in on pressing cybersecurity issues.

Title: The Dark Art of Alert Correlation: Extracting Attack Chains from Chaos

Tags: Middle Easterns & Africans in Cyber Security (MEACS) | Creator Talk/Panel

When: Sunday, Aug 9, 12:00 - 12:30 PDT

Where: LVCCW Level 1 Hall 3 1100 (Creator Stage 7) - [Map](#)

Description:

In modern cybersecurity, the ability to connect isolated security alerts into coherent, actionable attack chains is essential. However, traditional detection methods often struggle to contextualize vast amounts of security data, leaving slow and stealthy attacks undetected within a sea of noise and false positives. This talk introduces a novel approach using open-source AI models to map, cluster, and correlate security alerts in order to uncover coordinated attacks. Through clustering, knowledge graphs, and AI-driven correlation, this approach offers significant improvements in SOC (Security Operations Center) efficiency and effectiveness. We detail the methodology, open source tools, and results of this approach across diverse environments, including cloud, telecom, and industrial control systems.

SpeakerBio: Ezz Tahoun

Ezz Tahoun is an award-winning cybersecurity data scientist recognized globally for his innovations in applying AI to security operations.

He has keynoted, trained & presented at BlackHat US, Sector, MEA, Asia & EU, DEFCON, SANS Summits, all the top Bsides, Securityweek ICS Conference and GISEC among many others.

His groundbreaking work earned him a gold edison award and accolades from Yale, Princeton, Northwestern, NATO, Microsoft, and Canada's CSE.

At 19, Ezz began his PhD in Computer Sci at the Univ of Waterloo, quickly gaining recognition through over 20 influential papers and open-source tools.

His experience includes leading advanced AI security ops projects for Orange CyberDefense, Forescout, RBC, and Huawei US.

He holds certifications such as GIAC Advisory Board, aCCISO, CISM, CRISC, GCIH, CEH, PMP and GCP-Cloud Architect, and served as an adjunct professor in cyber defense and warfare.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: The Death of Dicom

Tags: Biohacking Village | Creator Talk/Panel

When: Saturday, Aug 8, 10:30 - 10:59 PDT

Where: LVCCW Level 1 Hall 3 1104 (Creator Stage 4) - [Map](#)

Description:

DICOM (Digital Imaging and Communications in Medicine) is the lingua franca of medical imaging — a decades-old protocol embedded in nearly every hospital network, PACS server, and imaging modality on the planet. It is also, by modern standards, a deeply permissive protocol: built on assumptions of trusted networks, sprawling parser surface area, and file formats that double as executable carriers. For an attacker, that combination is a gift. This talk explores how DICOM can be repurposed as offensive infrastructure across the full red team lifecycle. We'll walk through the protocol's exploitable design choices, demonstrate techniques for initial access, lateral movement, and persistence inside healthcare environments, and examine how DICOM files themselves can be abused as polyglot payload carriers that survive AV, EDR, and content inspection. Along the way, we'll look at real-world PACS deployments, the surprising reach of DICOM beyond hospitals, and why this protocol represents one of the largest under-examined attack surfaces in critical infrastructure today. Attendees will leave with a working mental model of DICOM from an offensive perspective, concrete TTPs they can incorporate into engagements against healthcare and adjacent verticals, and a healthy appreciation for why their next CT scan might be running on a Windows XP box.

SpeakerBio: Michael "v3ga" Aguilar, Principal Consultant at Sophos Red Team

Michael Aguilar (v3ga) is a Principal Consultant on the Sophos Red Team, paid to think like the people his clients are afraid of. His work lives at the intersection of offensive security, vulnerability research, and low-level systems programming, Windows internals, reverse engineering, and the kind of dusty attack surfaces that nobody has looked at since the protocol was ratified. Sometimes, he's lucky enough to perform full Physical Red teams against his client targets. His method is unglamorous and effective: Analyze, Formulate, Target, Attack (covertly).

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: The DEF CON 34 Badge

Tags: DEF CON Official Talk

When: Friday, Aug 7, 10:30 - 10:59 PDT

Where: LVCCW Level 1 Hall 3 1006 (Main Track 1) - [Map](#)

Description:

The badge: how it was made, how to hack it, the new open source chip powering it, and how you can use it as a hardware security token after the con! bunnie shares his experiences zero-shotting the badge with the help of team Cheeso.

This year's badge goes deeper into the open source rabbit hole than ever before. It features the Baochip-1x, a security-oriented "high-assurance" CPU that embraces Kerckhoffs's principle: not only can you check out most of the hardware design source, you can also directly see its transistors using infrared light. Learn more about how to unlock the power of open source silicon, and power up your hacking game with "God Mode" visibility into the heart of the machine.

SpeakerBio: Andrew 'bunnie' Huang

Andrew 'bunnie' Huang is best known for his work hacking the Microsoft Xbox, as well as for designing and manufacturing open source hardware. His current research interest is in facilitating trust in technology. He developed the IRIS (Infra-Red, In-Situ) imaging technique for silicon, and is the founder of Baochip, a fabless open source silicon company.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

The Diana Initiative - Saturday - 16:00-17:59 PDT

Title: The Diana Initiative - Open time

Tags: The Diana Initiative | Creator Event/Activity

When: Saturday, Aug 8, 16:00 - 17:59 PDT

Where: LVCCW Level 2 W209 (Diana Initiative) - [Map](#)

Description:

In our community room between our birds of a feather conversations, meetups, workshops, and talks we have open time where you can come in and hang out - we have games and puzzles and lego!

We also have our "Reference Desk", not the NFO desk, but a service for overwhelmed individuals. Our friendly volunteers at our reference desk can help you come up with a plan before going back out into DEF CON. The reference desk will work to find and connect you with the amazing events and communities at the conference, as well as in the community at large, that are best suited to your interests.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

The Diana Initiative - Sunday - 10:00-10:59 PDT

Title: The Diana Initiative - Open time

Tags: The Diana Initiative | Creator Event/Activity

When: Sunday, Aug 9, 10:00 - 10:59 PDT

Where: LVCCW Level 2 W209 (Diana Initiative) - [Map](#)

Description:

In our community room between our birds of a feather conversations, meetups, workshops, and talks we have open time where you can come in and hang out - we have games and puzzles and lego!

We also have our "Reference Desk", not the NFO desk, but a service for overwhelmed individuals. Our friendly volunteers at our reference desk can help you come up with a plan before going back out into DEF CON. The reference desk will work to find and connect you with the amazing events and communities at the conference, as well as in the community at large, that are best suited to your interests.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

The Diana Initiative - Sunday - 13:00-13:59 PDT

Title: The Diana Initiative - Open time

Tags: The Diana Initiative | Creator Event/Activity

When: Sunday, Aug 9, 13:00 - 13:59 PDT

Where: LVCCW Level 2 W209 (Diana Initiative) - [Map](#)

Description:

In our community room between our birds of a feather conversations, meetups, workshops, and talks we have open time where you can come in and hang out - we have games and puzzles and lego!

We also have our "Reference Desk", not the NFO desk, but a service for overwhelmed individuals. Our friendly volunteers at our reference desk can help you come up with a plan before going back out into DEF CON. The reference desk will work to find and connect you with the amazing events and communities at the conference, as well as in the community at large, that are best suited to your interests.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

The Diana Initiative - Friday - 12:00-12:59 PDT

Title: The Diana Initiative - Open time

Tags: The Diana Initiative | Creator Event/Activity

When: Friday, Aug 7, 12:00 - 12:59 PDT

Where: LVCCW Level 2 W209 (Diana Initiative) - [Map](#)

Description:

In our community room between our birds of a feather conversations, meetups, workshops, and talks we have open time where you can come in and hang out - we have games and puzzles and lego!

We also have our "Reference Desk", not the NFO desk, but a service for overwhelmed individuals. Our friendly volunteers at our reference desk can help you come up with a plan before going back out into DEF CON. The reference desk will work to find and connect you with the amazing events and communities at the conference, as well as in the community at large, that are best suited to your interests.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

The Diana Initiative - Saturday - 12:00-12:59 PDT

Title: The Diana Initiative - Open time

Tags: The Diana Initiative | Creator Event/Activity

When: Saturday, Aug 8, 12:00 - 12:59 PDT

Where: LVCCW Level 2 W209 (Diana Initiative) - [Map](#)

Description:

In our community room between our birds of a feather conversations, meetups, workshops, and talks we have open time where you can come in and hang out - we have games and puzzles and lego!

We also have our "Reference Desk", not the NFO desk, but a service for overwhelmed individuals. Our friendly volunteers at our reference desk can help you come up with a plan before going back out into DEF CON. The reference desk will work to find and connect you with the amazing events and communities at the conference, as well as in the community at large, that are best suited to your interests.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

The Diana Initiative - Friday - 14:00-14:59 PDT

Title: The Diana Initiative - Open time

Tags: The Diana Initiative | Creator Event/Activity

When: Friday, Aug 7, 14:00 - 14:59 PDT

Where: LVCCW Level 2 W209 (Diana Initiative) - [Map](#)

Description:

In our community room between our birds of a feather conversations, meetups, workshops, and talks we have open time where you can come in and hang out - we have games and puzzles and lego!

We also have our "Reference Desk", not the NFO desk, but a service for overwhelmed individuals. Our friendly volunteers at our reference desk can help you come up with a plan before going back out into DEF CON. The reference desk will work to find and connect you with the amazing events and communities at the conference, as well as in the community at large, that are best suited to your interests.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Physical Security Village - Friday - 16:00-16:30 PDT

Title: The Door Was Already Open

Tags: Physical Security Village | Creator Talk/Panel

When: Friday, Aug 7, 16:00 - 16:30 PDT

Where: LVCCW Level 1 Hall 3 1104 (Creator Stage 4) - [Map](#)

Description:

Physical access control systems are often assumed to be secure, but many rely on flawed design assumptions, and can contain misconfigurations. This talk examines a widely deployed platform, where internet-exposed panels, numeric-only passcodes, and predictable communication patterns enable remote discovery and access at mass scale. With no rate limiting or lockout protections, authentication can be automated, often succeeding due to default credentials, or an easily guessed combination. Successful access exposes sensitive data, including resident information, credentials, and access history. It also allows for complete remote control of the access control system. This talk focuses on how architectural decisions — not just bugs — can create systemic vulnerabilities in real-world security systems. Come on in, The Door Was Already Open.

SpeakerBio: Champ

Hello!! I am a Canadian Physical Security Consultant, who loves finding a new way to pop a door.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: The Dots Do Matter: Gmail's Invisible Blindspot

Tags: AppSec Village | Creator Talk/Panel | All Audiences

When: Friday, Aug 7, 10:30 - 10:59 PDT

Where: LVCCW Level 1 Hall 2 604 (Appsec Village) Main Stage - [Map](#)

Description:

In 2004, I registered kerene@gmail.com during Gmail's invite-only launch. I've been receiving strangers' private data ever since, without clicking a single link or running a single exploit. Gmail treats dots as invisible, meaning all 32 dot-variants of my address deliver straight to me. Alas, Third-party platforms never got the memo. Banks, airlines, social networks, and government portals mostly treat dot-variants as unique identities, creating an invisible identity collision with real consequences for account security, fraud, and forensic investigation, impacting millions of users worldwide. Almost 90 Snapchat log in emails, 168 TikTok password resets, and one Google Takeout link later, I'm here to show you what 22 years of someone else's data looks like, and the one normalization fix that would have prevented all of it.

SpeakerBio: Keren Elazari

Keren Elazari is an internationally recognized security analyst, researcher, author and speaker, working with leading security firms, government organizations and Fortune 500 companies. As an independent voice on cyber security, Keren Elazari is the first Israeli woman to give a TED talk at the official TED Conference. Keren's TED talk about hackers has been viewed by millions, translated to 30 languages and is one of the most watched talks on TED.com on the topic of cyber security. Keren is the founder of BSidesTLV, Israel's largest security community event, and the founder of the Leading Cyber Ladies network for Women in Cyber Security. Keren is currently a senior researcher at the Interdisciplinary Cyber Research Center at Tel Aviv University.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: The EFF Benefit Poker Tournament

Tags: The EFF Benefit Poker Tournament | Contest

When: Friday, Aug 7, 12:00 - 14:59 PDT

Where: Other / See Description

Description:

The EFF Benefit Poker Tournament is back for DEF CON 34! Your buy-in is paired with a donation to support EFF's mission to protect online privacy and free expression for all. Play for glory. Play for money. Play for the future of the web. Seating is limited, so reserve your spot today.

When: Friday, August 7, 2026 - 12:00-15:00

Where: Horseshoe Poker Room, 3645 S Las Vegas Blvd, Las Vegas, NV 89109

Tournament Specs: \$100 Horseshoe tournament buy-in, with a donation of \$250 or more to EFF to sign up. (AND all players will receive a complimentary EFF Gold Level Membership for the year.) Re-buys are unlimited to level 6, with each having a suggested donation of \$100 on site. Levels will be fifteen minutes, and the blinds go up at each level. Attendees must be 21+.

Pre-Tournament Clinic: Have a friend that might be interested but not sure how to play? Have you played some poker before but could use a refresher? Join poker pro Mike Wheeler (Tarah's dad) and celebrities for a free poker clinic from 11:00 am-11:45 am just before the tournament. Mike will show you the rules, strategy, table behavior, and general Vegas slang at the poker table. Even if you know poker pretty well, come a bit early and help out.

Emcee & Celebrity Guests: We'll have Celebrity Bounties again! Knock out a celebrity and get neat EFF swag and the respect of your peers! Plus, as always, knock out Tarah's dad Mike, and she donates \$250 to the EFF in your name!

The Celebrities: This year's event will feature many of our legal celebrities in our Legal Champions Edition edition.

The Glory: The tournament winner will receive the traditional Jelly Bean Trophy and we hope you'll like this year's newest add: We will have bug bounty pins this year! When you take someone out of the tournament, they will give you a pin. Prizes—and major bragging rights—go to the player with the most bounty pins.

Speakers: Cindy Cohn, Jennifer Granick, Marcia Hofmann, Kurt Opsahl, Liz Wharton

SpeakerBio: Cindy Cohn, Executive Director at Electronic Frontier Foundation

Cindy Cohn is the Executive Director of the Electronic Frontier Foundation. From 2000-2015 she served as EFF's Legal Director as well as its General Counsel. Ms. Cohn first became involved with EFF in 1993, when EFF asked her to serve as the outside lead attorney in *Bernstein v. Dept. of Justice*, the successful First Amendment challenge to the U.S. export restrictions on cryptography. Ms. Cohn is the author of the professional memoir, called *Privacy's Defender* published by MIT Press in March, 2026. She is also the co-host of EFF's award-winning podcast, *How to Fix the Internet*.

--

Cohn first became involved with EFF in 1993, when EFF asked her to serve as the outside lead attorney in *Bernstein v. Dept. of Justice*, the successful First Amendment challenge to the U.S. export restrictions on cryptography. She served as EFF's Legal Director as well as its General Counsel from 2000 through 2015, and she has served as Executive Director since then. She also has co-hosted EFF's award-winning "How to Fix the Internet" podcast, which recently concluded its sixth season. Her professional memoir covering her time at EFF, *Privacy's Defender: My Thirty-Year Fight Against Digital Surveillance*, was published earlier this year by MIT Press.

SpeakerBio: Jennifer Granick, Hacker lawyer 1.0

Throughout her career, Jennifer Granick has fought for civil liberties in an age of massive surveillance and powerful digital technology. As the former surveillance and cybersecurity counsel with the ACLU Speech, Privacy, and Technology Project, she litigated, spoke, and wrote about privacy, security, technology, and constitutional rights. Granick is the author of the book *American Spies: Modern Surveillance, Why You Should Care, and What To Do About It*, published by Cambridge Press and winner of the 2016 Palmer Civil Liberties Prize.

SpeakerBio: Marcia Hofmann, Founder and Principal at Zeitgeist Law

Founder and principal of Zeitgeist Law, a boutique law firm focused on information security, computer crime, electronic privacy, free expression, and intellectual property issues. In the past, she has worked at Twitter, the Electronic Frontier Foundation, and the Electronic Privacy Information Center. She was a US-UK Fulbright Cyber Security Scholar based at the University of Oxford, where she studied educational and restorative justice programs for young computer crime offenders. She has taught courses in computer crime at Colorado Law and Internet law at UC Law San Francisco (then known as UC Hastings).

SpeakerBio: Kurt Opsahl, Associate General Counsel for Cybersecurity and Civil Liberties Policy at Filecoin Foundation

Kurt Opsahl is the Associate General Counsel for Cybersecurity and Civil Liberties Policy for the Filecoin Foundation. Formerly, Opsahl was the Deputy Executive Director and General Counsel of EFF. Opsahl was also the lead attorney on the Coders' Rights Project, and continues to assist EFF with that work.

SpeakerBio: Liz Wharton, Founder at Silver Key Strategies

Elizabeth (Liz) Wharton leverages two decades of legal, public policy, and business experience to build and scale cybersecurity and threat intelligence focused companies. Prior experience includes leading a third-party risk threat intelligence platform startup and serving as Atlanta's Senior Attorney overseeing technology policy and projects for the Airport and on it's ransomware incident immediate IR team. Awarded the 2022 "Cybersecurity or Privacy Woman Law Professional of the Year" by the United Cybersecurity Alliance, Liz volunteers as a mentor and for the Rural Technology Fund (Board member), ICS Village's Hack the Capitol (Planning Committee), and DEFCON (CFP Review Board). She received her JD from Georgia State University and her BA from Virginia Tech.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: The Enclave is Lying to You: Breaking TEE Trust Boundaries Through Boot-Time State

Tags: DEF CON Official Talk | Demo | Tool

When: Saturday, Aug 8, 14:00 - 14:59 PDT

Where: LVCCW Level 1 Hall 3 906 (Main Track 3) - [Map](#)

Description:

Confidential computing on cloud TEEs: Nitro Enclaves, SEV-SNP, and TDX promises that a fully compromised host cannot reach into a hardware-isolated enclave. The cryptographic attestation story holds. The deployment story does not.

This talk demonstrates attacks that bypass TEE isolation without touching the enclave image. We target the inputs an enclave trusts at boot: cloud object storage, host-supplied environment variables, and KMS keys whose policies forget to enforce attestation. None are covered by attestation. All reach inside.

We demonstrate remote code execution as root inside a Nitro Enclave with a single s3:PutObject permission. No host access. No SSH. One file upload containing a path traversal, one boot cycle, and the enclave executes attacker-controlled code.

From inside we intercept KMS decrypts live to extract the database encryption key in plaintext, exfiltrate the enclave's IAM credentials, and establish persistence across reboots without re-exploitation - all while PCR measurements remain unchanged and attestation reports a healthy enclave.

We release an open-source auditing tool, walk through which defenses held, and provide a hardening checklist for any team running workloads inside TEEs.

The enclave isn't broken. The way we deploy it is.

AWS, "AWS Nitro Enclaves User Guide," <https://docs.aws.amazon.com/enclaves/latest/user/nitro-enclave.html> AWS, "Cryptographic Attestation with AWS KMS for Nitro Enclaves," <https://docs.aws.amazon.com/kms/latest/developerguide/services-nitro-enclaves.html> A. Tsow, "Attacking Confidential Computing: A Survey of TEE Exploitation Techniques," IEEE S&P Workshop on Offensive Technologies (WOOT), 2024 NCC Group, "Public Report - AWS Nitro System Security Review," 2023, <https://research.nccgroup.com/2023/04/Trail-of-Bits-Security-Assessment-of-AWS-Nitro-Enclaves/> 2022 MITRE ATT&CK, "Cloud Matrix - Initial Access / Valid Accounts," <https://attack.mitre.org/techniques/T1078/004/> J. Aas et al., "Understanding TEE Trust Models in Cloud Deployments," USENIX Security Symposium, 2023 OWASP, "Path Traversal," https://owasp.org/www-community/attacks/Path_Traversal AWS, "Instance Metadata Service Version 2 (IMDSv2)," <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/configuring-instance-metadata-service.html> Apache Thrift Project, "Thrift Binary Protocol Specification," <https://github.com/apache/thrift/blob/master/doc/specs/thrift-binary-protocol.md>

SpeakerBio: Sandeep "pyro" Jayashankar, Independent Researcher

Sandeep Jayashankar is a security researcher specializing in offensive security and adversarial simulations. His work spans AWS, Azure, and GCP environments, with current research focused on trusted execution environment exploitation, confidential computing trust boundaries, and the security of AI/ML systems deployed in cloud-native architectures. This research was conducted under an authorized adversarial simulation program. He approaches security research from a defender's perspective: every offensive finding ships with a concrete, auditable control that defenders can deploy. He previously presented at RSA Conference 2025.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: The Enshittified Internet and How We Can All Rewild the Internet

Tags: Hackers.town | Creator Talk/Panel

When: Sunday, Aug 9, 10:30 - 10:59 PDT

Where: LVCCW Level 1 Hall 3 1100 (Creator Stage 7) - [Map](#)

Description:

The Internet was once a place where people could talk, share ideas and knowledge, express themselves with personal websites, build communities, and more. In recent years, however, we have seen that magic fade away, as the internet of today is now a toxic cesspool of social media controlled by Big Tech, ads thrown everywhere, walled gardens, AI generated slop, and content that locks us in by making us angry and depressed. This is not the Internet we need or should leave to the next generation of hackers! There are ways to take back and rewild the web! This talk is part informative, part education, part historical, and pure hacker punk energy as we explore how to do things like self-host our own servers, tools we can use to build new networks, decentralized services for communication, media sharing, and more, old protocols and services us old timers used to use that still exist (and how the kids can use them, too!), and places and sites we can go to for the education and information we want! In all, this talk is about hacking the planet and taking our Internet... the people's Internet... back from corporate corruption and control!

SpeakerBio: LambdaCalculus

LambdaCalculus is chaos in a trenchcoat, and is passionate to his core about human rights issues, community outreach, and education. He has spoken at HOPE in 2025 on the Pirate Box and Sneakernet, and has also spoken at DEF CON, JawnCon, and PhreakNIC. He is a member of hackers.town, a native of the NYC area, and can still hit a mosh pit! Find him hanging out at hackers.town on Mastodon:<https://masto.hackers.town/@LambdaCalculus>

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Hackers.town - Saturday - 15:00-15:59 PDT

Title: The Enshittified Internet and How We Can All Rewild the Internet

Tags: Hackers.town | Creator Talk/Panel

When: Saturday, Aug 8, 15:00 - 15:59 PDT

Where: LVCCW Level 1 Hall 4 1420 (Hackers.town) - [Map](#)

Description:

SpeakerBio: LambdaCalculus

LambdaCalculus is chaos in a trenchcoat, and is passionate to his core about human rights issues, community outreach, and education. He has spoken at HOPE in 2025 on the Pirate Box and Sneakernet, and has also spoken at DEF CON, JawnCon, and PhreakNIC. He is a member of hackers.town, a native of the NYC area, and can still hit a mosh pit! Find him hanging out at hackers.town on Mastodon:<https://masto.hackers.town/@LambdaCalculus>



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Red Team Village - Friday - 10:00-10:59 PDT

Title: The Entropy Illusion: High-Speed Cracking on a Budget

Tags: Red Team Village | Misc

When: Friday, Aug 7, 10:00 - 10:59 PDT

Where: LVCCW Level 1 Hall 1 309 (Red Team Village) Workshop Tactic Table 5 - [Map](#)

Description:

As modern password policies mandate 14+ characters, defenders have developed a false sense of security while red teams have entered a costly hardware arms race. But length is not the same as entropy. As policies grow stricter, human behavior becomes more predictable.

This session will demonstrate approaches focusing on high yielding results within a limited testing time frame and budget. We will explore tactics for leveraging custom probability masks, dictionary slicing and exploiting human predictability to prove brains still win over GPU's.

SpeakerBio: Chris Claunch

CMIYC competitor (Team Cynosure Prime) 10+ years Red Teaming



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: The Front Lines Need Detection Engineers : Would You Like to Know More?

Tags: Noob Community | Creator Talk/Panel

When: Friday, Aug 7, 16:35 - 17:05 PDT

Where: LVCCW Level 1 Hall 4 1417 (Noob Community) - [Map](#)

Description:

Would You Like to Know More? Becoming a Detection Engineer

Detection Engineering is one of the fastest-growing specialties in cybersecurity. But what does a Detection Engineer actually do?

In this beginner-friendly lightning talk, I'll share how I stumbled into Detection Engineering, what the job really looks like, the skills that mattered most, and the mistakes I wish I'd avoided. Whether you're a SOC analyst, student, or simply curious about the field, you'll leave with a clearer understanding of the role and practical steps to begin your own journey.

Citizenship not required. Curiosity mandatory.

SpeakerBio: Kyle Barboza

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Bug Bounty Village - Friday - 10:00-10:59 PDT

Title: The Future of Bug Bounty - Program Manager Perspective

Tags: Bug Bounty Village | Creator Talk/Panel

When: Friday, Aug 7, 10:00 - 10:59 PDT

Where: LVCCW Level 1 Hall 3 1102 (Creator Stage 6) - [Map](#)

Description:

Bug bounty is a proven model, but AI is changing how it runs. Researchers are submitting at higher volumes, LLM-generated reports are making triage harder, and new assets like AI agents and model endpoints are showing up in scope faster than programs can write playbooks for them. This panel brings together program managers from leading bug bounty programs to talk about what they're seeing from the other side of the queue. What has AI actually changed about the reports, the researchers, and the bugs that matter? What should program managers and security teams be doing about it now? And where is bug bounty headed over the next few years? Whether you run a program, hack on one, or want to start one, you'll come away with a clearer sense of what bug bounty looks like today and where it is going.

Speakers: Jai Kumar Sharma, Catherine Cassell, Austin Sturm, Dane Sherrets, Sachin "sachinnthakuri" Thakuri

SpeakerBio: Jai Kumar Sharma, Principal Offensive Security Engineer at GoDaddy

Jai Sharma is a Principal Offensive Security Engineer at GoDaddy, where he leads cloud penetration testing, red team operations, AI red teaming, and security research across one of the world's largest domain registrars and hosting platforms. A self-taught offensive security researcher from New Delhi, India, he built his career with a hacker's mindset, breaking code logic, chasing vulnerabilities, and proving real-world business impact from technical exploits. He also leads TTP research, drives threat emulation efforts, and works closely with blue teams to sharpen detection through an adversary-focused lens.

At GoDaddy, Jai tests the same infrastructure and enterprise environments that millions of customers rely on. His work spans cloud and on-premises penetration testing, IAM privilege escalation research, and building automated offensive tooling that helps turn point-in-time assessments into continuous detection. Before GoDaddy, Jai held offensive security roles at Housing.com, FIS, and EY, giving him firsthand experience with how security weaknesses and misconfigurations surface across different industries, architectures, and maturity levels.

Jai volunteers with the DEF CON community as CTF Ops for the Cloud Village and on-site Coordinator for the Bug Bounty Village.

SpeakerBio: Catherine Cassell, Product Security Engineer at Github

Catherine is a security engineer on the bug bounty team at GitHub. She has five years of experience in offensive security, working in both bug bounty and penetration testing. Catherine has spent the last year and a half at GitHub and runs an annual hardware hacking workshop at the Glass Firewall Conference. At work, she spends her days reading and triaging bounty reports. Outside of work, she spends her free time outside, as far away from screens as possible. You can usually find her hiking or skiing in the Rocky Mountains.

SpeakerBio: Austin Sturm

He started as a no-good kid on IBB forums and landed a job doing offensive security for large tech companies. For some tireless years he ran and built a team for a cloud providers bug bounty program and continues to act as a tech lead for a bounty program in the wake of the AI-era

SpeakerBio: Dane Sherrets, HackerOne

Dane is an Innovations Architect at HackerOne, where he helps organizations run AI-focused bug bounty programs and improve the security of emerging technologies. His work includes winning 2nd place in the Department of Defense AI Bias Bounty competition, discovering critical vulnerabilities in platforms like Worldcoin, and helping design and manage Anthropic's AI Safety Bug Bounty program. Drawing on his background as a bug hunter, Dane blends strategic guidance with hands-on expertise to advance the safety and security of disruptive tech across industries.

SpeakerBio: Sachin "sachinnthakuri" Thakuri, Senior Product Security Engineer at TikTok

Sachin Thakuri is a Senior Product Security Engineer at TikTok, where he leads Variant Analysis initiatives to identify and eliminate classes of vulnerabilities across the platform. His work focuses on variant analysis, vulnerability management, product incident response, and building AI-powered security tooling. Previously, Sachin help build and led application security programs at Alpha Group, Pintu, and Grab. Sachin has also presented his research at security conferences like Black Hat, Insomni'hack, GreHack.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: The Future of Payments: AI, Agentic Commerce and the Next Wave of Innovation

Tags: Payment Village | Creator Talk/Panel

When: Friday, Aug 7, 10:45 - 11:30 PDT

Where: LVCCW Level 1 Hall 3 1104 (Creator Stage 4) - [Map](#)

Description:

The payments industry is entering a new era of transformation, where AI reshapes the way consumers and businesses buy, pay, and determine risk throughout the payment journey.

Join leaders from across the payments ecosystem as they explore the technologies, opportunities, and challenges shaping the future of this space. This panel will examine how financial institutions, payment providers, merchants, and technology companies are preparing for a world where AI augments decision-making, automates operations, and increasingly acts on behalf of users to deliver more seamless, secure, and intelligent payment experiences.

Attendees will gain actionable insights into the technologies and market forces redefining payments. Panelists will share their perspectives on the emerging innovations, strategic priorities, and industry shifts that will shape the next generation of payment experiences. They will offer practical guidance on how organizations can prepare for an increasingly intelligent, automated, and interconnected payments ecosystem.

Speakers: Daniel Cuthbert, Leigh-Anne Galloway, Jorge Braniff, Sanjeev Sharma

SpeakerBio: Daniel Cuthbert, Global Head of Cyber Security Research, Banco Santander

Daniel Cuthbert is the Global Head of Cyber Security Research at Santander, where he leads global security research and drives innovation in cyber defence across the organisation. He serves on the Black Hat Review Board and is a founding member of OWASP, having co-authored both the OWASP Testing Guide and the OWASP Application Security Verification Standard (ASVS). With more than 20 years of experience in offensive security, application security, and threat research, Daniel is a frequent speaker and trusted advisor on emerging cyber threats, secure engineering, and security strategy.

SpeakerBio: Leigh-Anne Galloway, Founder, Payment Village

Leigh-Anne Galloway is a security researcher and testing specialist focusing on payment security, application security, fraud, and adversarial testing. Leigh-Anne is the founder of The Payment Village, a non-profit initiative dedicated to educating people on the intricacies of payment systems, fostering the next generation of payment security professionals, and creating space for critical discussion within the industry. She has presented and authored research on ATM security, mPOS vulnerabilities, NFC payments, fraud, and application security.

SpeakerBio: Jorge Braniff, VP of Fraud and Product Operations at Incode Technologies

Jorge Braniff is VP of Fraud and Product Operations at Incode Technologies, where he leads a global organization spanning fraud detection, document intelligence, red team, data collection, labeling and identity verification. His work sits at the center of the agentic fraud arms race: partnering with ML on the development of models for supporting all ID templates, deepfake detection, presentation attacks, document tamper, alteration, liveness and AI detection. Jorge has led fraud ring detection initiatives using graph-based identity linkage to uncover coordinated attack networks and has run high-stakes technical evaluations against fraud rings targeting neobanks and payment platforms. He has also hardened SDKs against injection and deepfake-based attacks for major financial institutions and fintechs and developed model governance and evaluation frameworks used to benchmark fraud detection performance in production. He brings a builder's perspective to the fight against AI-driven fraud, having scaled operations and detection systems across multiple countries. He is based in the San Francisco Bay Area.

SpeakerBio: Sanjeev Sharma, Director, Payments Product, GoFundMe

Sanjeev has been building payment products since 2013, beginning his career at Visa as part of the original Visa Token Service (VTS) product team. He played a key role in launching and commercializing VTS across multiple countries and continents, helping drive the adoption of tokenized payments at global scale. He later joined Meta, where he worked on payments across the family of apps, including helping launch WhatsApp Payments in India. Today, Sanjeev is a Product Manager in the Payments Product Group at GoFundMe, where he focuses on building secure, scalable payment experiences that help people support one another around the world.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: The Ghost Key: Illusions of "Time Management" in TTLock Smart Locks

Tags: DEF CON Official Talk | Demo | Tool | Exploit

When: Saturday, Aug 8, 10:00 - 10:59 PDT

Where: LVCCW Level 1 Hall 3 1006 (Main Track 1) - [Map](#)

Description:

Smart locks are widely used in rental, hotel, and residential markets. As a major provider, TTLock (Sciener) operates in over 200 countries and relies on Offline Time Management to issue temporary eKeys without network access. However, our research reveals critical security flaws in this common offline design. From real-world anomalies, we analyzed TTLock's proprietary BLE protocol and found serious weaknesses in its cryptographic verification and authentication. Lacking proper validation, the so-called secure offline architecture is fully bypassable. We uncovered three critical design flaws: full revocation bypass, expired credential resurrection, and low-cost DoS. In this talk, we will demonstrate exploitation with a Mac and custom Python tools. We show that time management in TTLock is a mere illusion, turning physical security into an open digital door.

Speakers: Yang Liu, Zhenghan Wang

SpeakerBio: Yang Liu, Hillstone Networks Co., Ltd.

Yang Liu is a Security Researcher at Hillstone Network Security Research Institute, specializing in binary vulnerability hunting, ICS security, mobile security, and reverse engineering. With extensive experience in both red-teaming and defense, Yang has discovered numerous vulnerabilities in complex industrial control systems. He is a frequent speaker in the security community, notably presenting his ICS research at the Kanxue Security Development Conference (SDC). An avid CTF competitor, Yang excels in Reverse Engineering, Mobile, and ICS categories. He also leverages his real-world combat experience to provide professional cybersecurity training for enterprises.

SpeakerBio: Zhenghan Wang, Hillstone Networks Co., Ltd.

Zhenghan Wang is a security researcher focusing on IoT security and open-source software security. His research interests include embedded system security, protocol analysis, reverse engineering, and vulnerability discovery. He is dedicated to finding and disclosing real-world security issues to help improve the safety of connected devices and open-source projects.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: The Glass Perimeter: Systematic Bypasses in Biometric Frameworks and the Rise of Synthetic Identity

Tags: DEF CON Official Talk | Demo | Exploit

When: Saturday, Aug 8, 12:00 - 12:59 PDT

Where: LVCCW Level 1 Hall 3 906 (Main Track 3) - [Map](#)

Description:

Identity is the new perimeter, and biometrics are its supposed gatekeepers. But what happens when the gatekeepers are blind to the reality they consume? We spent more than 6 months deconstructing the biometric "Root of Trust" across every top-tier framework we could find, solutions relied upon by the world's largest banks and providers worth billions. The result: A 100% bypass rate. From high-fidelity physical spoofs to a first-of-its-kind Cross-PID buffer hijack against integrated anti-tamper SDKs, we prove that even multi-million dollar "fortresses" can be reduced to client-side theater. This talk is a technical journey through the guts of the mobile media pipeline, exposing how synthetic identities are manufactured at scale to bypass RASP, Kernel-level integrity, and AI models. When the "Master Key" is just another line of code an attacker can hook, the risk isn't just a bug, it's a systemic failure affecting millions of users. Customers are losing wealth, companies are buying illusions, and the glass perimeter is shattering.

Speakers: Dan Borgogno, Javier Bernardo

SpeakerBio: Dan Borgogno, Security Researcher at Faraday

Dan Borgogno is a security researcher, backend developer, security engineer and international speaker with years of experience on mobile, hardware, IoT and web application hacking.

SpeakerBio: Javier Bernardo, Strike Security

Senior Pentester, Security Engineer and Cybersecurity Researcher (+15 years) with a wide area of expertise in Offensive Security and Red Team. Passionate Bug Hunter and self-taught Cybersecurity Specialist who loves to hack almost everything.

Organizer of Bug Bounty Argentina Community: <https://twitter.com/BugBountyArg> Speaker and Organizer at Ekoparty Security Conference: <https://ekoparty.org/>

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: The Hard Part of ASM: Ownership Attribution

Tags: Recon Village | Creator Workshop

When: Saturday, Aug 8, 12:40 - 15:10 PDT

Where: LVCCW Level 1 Hall 2 501 (Recon Village) - [Map](#)

Description:

Attack Surface Management (ASM) lives or dies on a deceptively simple question: who owns this? Without reliable attribution, an asset inventory is just a pile of hosts, domains, certificates, and cloud endpoints—with no defensible way to scope an organization’s true digital footprint or separate first-party infrastructure from vendors, subsidiaries, acquisitions, joint ventures, and brand portfolios.

This talk dives into the real-world challenge of attributing internet-exposed assets to legal entities, not just names. Corporate identity is messy: organizations operate under trade names, localized spellings, legacy names, and jurisdiction-specific registrations. Meanwhile, the internet leaks ownership signals through fragmented, lossy metadata—RDAP/WHOIS, certificate subject/issuer fields, ASN registrations, DNS TXT verification records, trademark references, and public corporate registries. Each source is incomplete on its own; together they can still conflict, drift over time, and create duplicate “identities” that quietly degrade attribution accuracy.

Using the OWASP Amass Project as a concrete reference point, we’ll walk through an attribution-centric discovery workflow: collecting signals, normalizing entity identity, resolving aliases across jurisdictions, and scoring confidence to decide when to merge, when to split, and when to escalate for analyst review. We’ll also explore how attribution errors propagate into ASM outcomes—missed scope, false positives, and blind spots in third-party exposure—and how disciplined entity modeling can turn noisy OSINT into a repeatable system of record.

Attendees will leave with practical techniques for improving attribution quality, a mental model for entity resolution, and actionable ideas for making ASM outputs trustworthy enough to drive risk decisions.

SpeakerBio: Jeff Foley, Founder and Project Leader at OWASP Amass Project

No BIO available

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: The Hidden Cost of Agentic Connectivity

Tags: Cloud Village | Creator Talk/Panel

When: Friday, Aug 7, 13:20 - 13:59 PDT

Where: LVCCW Level 3 W313 (Cloud Village Talks) - [Map](#)

Description:

During our extensive research on MCP servers, we uncovered critical vulnerabilities that pose significant risks to the cloud infrastructure management. These vulnerabilities enable malicious actors to interact with and compromise organizational infrastructure. Alarming, while some MCP servers had implemented protective measures against such misuse, these measures were often flawed, allowing for trivial bypasses.

In this presentation, we will underscore the necessity of comprehensive visibility and robust policy guidelines for every organization. Our analysis of over 19,000 MCP servers reveals substantial gaps and vulnerabilities within the so-called security features of these systems. We will demonstrate how these security features can be bypassed and highlight the real-world implications of these vulnerabilities.

Through active scanning, we identified the same vulnerable MCP server implementations deployed in the wild, confirming that these vulnerabilities are actively exploitable. This underscores the urgent need for organizations to adopt a strategic approach to managing MCP servers.

Our aim is for attendees to understand the critical importance of AI security beyond mere vulnerability management. Our findings show that even if the MCP server is not vulnerable, default deployments often introduce significant risks to organizational security. We will conclude our presentation by outlining best practices for mitigating the risks associated with MCP servers, ensuring that attendees leave with actionable insights to enhance their organization's security posture.

Speakers: David Fiser, Amy McMahon

SpeakerBio: David Fiser

David Fiser is a cybersecurity professional with over 15 years of experience. He regularly contributes to blogs and co-authors whitepapers on various security topics. He has been credited with several CVEs, including high-profile vendors such as Microsoft and NVIDIA. He presented his previous research at multiple security conferences. Personally, David is passionate about motorsport, cars, planes, and motorcycles. He also likes fixing broken items and traveling.

SpeakerBio: Amy McMahon

Amy is a seasoned Systems Engineer with 20 years of experience supporting enterprise customers through the evolution of TippingPoint spanning its tenures under 3Com, Hewlett Packard Enterprise, and Trend Micro. With deep expertise in network security and intrusion prevention, Amy has built a reputation for translating complex network security challenges into actionable solutions for large-scale enterprise environments. Currently serving as a Subject Matter Expert in Networking Solutions at TrendAI, Amy brings both technical depth and strategic perspective to emerging AI-driven security challenges. She holds multiple industry certifications including CISSP, CEH, and AWS Solutions Architect, reflecting her commitment to staying at the forefront of network cybersecurity and cloud architecture.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: The Hidden Data Supply Chain: How a SaaS Platform Broadcast Credentials and Customer Identities

Tags: Middle Easterns & Africans in Cyber Security (MEACS) | Creator Talk/Panel

When: Saturday, Aug 8, 14:00 - 14:59 PDT

Where: LVCCW Level 1 Hall 4 1306 (Middle Easterns & Africans in Cyber Security (MEACS) Community) - [Map](#)

Description:

Security researcher Sam Jadali, known for uncovering DataSpii, presents new research on the hidden and often inadvertent data supply chains inside SaaS platforms. In controlled tests of Klaviyo, a marketing/CRM platform processing roughly 8 billion customer profiles across 600k+ websites, simply viewing a contact's profile transmitted that person's name, email, or identifier to outside vendors, several not on Klaviyo's sub-processor list. Worse, during account registration a test account's password, email, phone number, and company details were sent to 31 third-party hostnames including Google, Meta, and LinkedIn, with four endpoints reflecting the password back to confirm receipt. Some recipients hid behind unbranded domains that customers and compliance teams can't identify through ordinary inspection. As human- and AI-generated code ships faster, one small HTML flaw can broadcast sensitive data across supply chains few organizations monitor. Jadali walks through the evidence, reproducible from network captures and public Common Crawl records.

SpeakerBio: Sam Jadali

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: The impact of CTF Write-Ups

Tags: Noob Community | Creator Talk/Panel

When: Friday, Aug 7, 15:00 - 15:15 PDT

Where: LVCCW Level 1 Hall 4 1417 (Noob Community) - [Map](#)

Description:

Over three years I've published 150+ write-ups on CTF challenges. Along the way the write-ups stopped being just documentation and started being the most valuable thing I produce — sourcing job offers, collaborations, and credibility I never directly asked for. This talk makes the case that a write-up is not the report of your work but the work itself: where learning consolidates and reputation compounds. I'll share the concrete payoff, the craft, lessons learned, and a blueprint anyone can start with. No novel 0-day, just maybe the most underrated force multiplier in offensive cyber security.

SpeakerBio: Mathias Detmers

No BIO available

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Noob Community - Saturday - 10:30-10:45 PDT

Title: The importance of Networking in Cybersecurity community

Tags: Noob Community | Creator Talk/Panel

When: Saturday, Aug 8, 10:30 - 10:45 PDT

Where: LVCCW Level 1 Hall 4 1417 (Noob Community) - [Map](#)

Description:

Quick session on how important it is to network with other professionals, students, and vendors to gain knowledge, collaborate for defenses and also for career growth

SpeakerBio: Michael Lenz

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Social Gatherings/Events - Friday - 19:00-21:59 PDT

Title: The KEVOPS Sellout Pool Party II: Sponsored by Zyn

Tags: Party

When: Friday, Aug 7, 19:00 - 21:59 PDT

Where: Sahara Hotel Azul Ultra Pool - [Map](#)

Description:

The Sellout Pool Party is back. Join us for tacos and music!



[Return to Index](#) - Add to Google

- ics [Calendar](#) file

Lockpick Village - Sunday - 11:00-11:45 PDT

Title: The Knox Box - A Brief History(Part II)

Tags: Lockpick Village | Creator Talk/Panel

When: Sunday, Aug 9, 11:00 - 11:45 PDT

Where: LVCCW Level 1 Hall 1 407 (Lockpick Village) - [Map](#)

Description:

An enhanced version of the DC33 talk, with more information

SpeakerBio: Matthew O'Reilly

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: The Liability Stack: When Code Becomes Conduct

Tags: Policy @ DEF CON | Creator Talk/Panel

When: Friday, Aug 7, 14:00 - 14:30 PDT

Where: LVCCW Level 1 Hall 3 801 (Creator Stage 1) - [Map](#)

Description:

The legal question of when publishing code creates responsibility for downstream harm has never been fully settled, but the practical separation between writing code and being treated as responsible for its downstream use is breaking down across AI, crypto, cybersecurity, and platform law. Courts and regulators are increasingly reaching contradictory conclusions about structurally similar systems: autonomous agents acting on third-party platforms, open-source developers accused of operating financial infrastructure, secure-by-design evolving into reasonable-care expectations, and recommendation systems reframed as product design rather than publication. This talk maps common doctrinal tension underneath those debates and argues that traditional legal categories fail when control, deployment, and operation are distributed across maintainers, deployers, validators, governance participants, and autonomous systems. Rather than focusing on labels like developer or platform, it proposes a functional framework centered on control, participation, foreseeability, and proximity to harm. The current incoherence is itself becoming a systemic risk, and the people building these systems should help shape the framework before courts finish improvising one for them.

SpeakerBio: Carole House, Penumbra Strategies

Carole House is a strategic technology executive who has spent her career focusing on leveraging innovative technologies to combat national security threats. She is the founder and CEO of a strategic technology and national security advisory practice, Penumbra Strategies, senior advisor to New Vista Capital, Member of the California Innovation Council, and serves as a Distinguished Senior Fellow at the Association for Certified Anti-Money Laundering Specialists (ACAMS) and a Senior Fellow at the Atlantic Council GeoEconomics Center. Carole recently served as the White House National Security Council (NSC) as Special Advisor for Cybersecurity and Critical Infrastructure and Director for Cybersecurity and Secure Digital Innovation. During her time at the White House, Carole architected two Executive Orders driving critical steps to promote innovation in cybersecurity, digital identity, artificial intelligence, and digital assets. Carole has held positions in venture capital and served on corporate and advisory boards for three financial regulatory agencies, three non-profits, and an AI and quantum security startup. Carole's prior government experience includes service as a U.S. Army Captain and across the White House, Senate Homeland Security Committee, and the U.S. Treasury.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Blue Team Village - Friday - 15:45-16:45 PDT

Title: The Modern Detection Engineer

Tags: Blue Team Village | Creator Talk/Panel

When: Friday, Aug 7, 15:45 - 16:45 PDT

Where: LVCCW Level 2 W217 (Blue Team Village) Main Stage - [Map](#)

Description:

Detection Engineering is a concept rooted in decades of blue teaming, but applied with a modern lens. At its core, it's a practice where a blue teamer can apply principles across software engineering, security analysis, and data science to detect and respond to threats without needing to staff a traditional SOC. In 2026, this field is in the spotlight due to the meteoric growth of technology and AI, but like any field in security, it has its sharp edges and broken promises.

In this panel, we will discuss Detection Engineering in 2026 with a diverse set of experts who work on these problems every day. We will cover topics around threat research and hunting, writing and maintaining a ruleset, modern CI/CD practices for blue teams & codifying incident response in security operations.

Speakers: Alex Hurtado, Chase Phelps, Chris Kulakowski, Christina Parry, Zack Allen

SpeakerBio: Alex Hurtado

Alex Hurtado spent years using, tuning, and implementing SIEMs across Fortune 500s and startups alike before landing as Head of Detection Strategy at Nebulock. She builds content on SIEM and detection engineering and hosts Detection Engineering Dispatch, a podcast bringing detection engineers together to compare notes and move the space forward.

SpeakerBio: Chase Phelps

Chase Phelps is a Senior Detection Engineering Manager at Marsh, leading detection, response automation, and AI/ML tooling for a large-scale SOC. He started his career in the IT space, working roles from Desktop support to System Engineer. He made the jump to Security starting in the SOC before making the move to Detection Engineering. Outside of work, he's likely to be found in the gym, on the golf course, or playing Old School Runescape.

SpeakerBio: Chris Kulakowski

Chris Kulakowski is a driven technologist, innovator, and tinkerer of all things. His career spans across 15 years of Digital Media, Information Technology, Security Operations, Threat Intelligence and Digital Forensics roles. He is currently a senior technical staff member specializing in threat detection at IBM, supporting IBM internal businesses. Prior to IBM he held various roles at General Motors and Optiv. He is seasoned in responding to incidents, developing new threat detection content, and an expert in EDR technology.

Chris holds a Computer Criminology degree from Florida State University and several industry leading cyber security and digital forensics certifications including CISSP, EnCE, GCFE, GREM, GMON and Security+. Chris is also accredited with a Stanford University Advanced Computer Security Certificate and a member of the GIAC Advisory Board and author of 3 US patents.

SpeakerBio: Christina Parry

Christina Parry is a Staff Security Engineer at Huntress and a technical leader with 9+ years in tech and security, specializing in detection engineering, automation, and open-source software. She's experienced in building high-impact, scalable software solutions that automate everyday security workflows and elevate detection and response teams. Before Huntress, she was a Detection Engineer at Twitter and a member of the Threat Hunt team at Morgan Stanley. Christina is a mentor and ally for

underrepresented groups in security, and sometimes comes out of her shell to nerd out about the things she cares about.

SpeakerBio: Zack Allen

Zack has been in the security field for 14 years. He started as a contractor for the Air Force then moved into the startup world before landing at Datadog. At Datadog, he built the security research and labs department and grew their security products and threat detection programs.

He is also the creator of Detection Engineering Weekly, a Substack dedicated to detection engineering, incident response & threat intelligence.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Crypto & Privacy Village - Saturday - 17:00-17:59 PDT

Title: The National Fight Against ALPRs

Tags: Crypto & Privacy Village | Creator Talk/Panel

When: Saturday, Aug 8, 17:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 3 1104 (Creator Stage 4) - [Map](#)

Description:

Speakers: Freddy Martinez, Sarah

SpeakerBio: Freddy Martinez

No BIO available

SpeakerBio: Sarah

Sarah has been working at the EFF on building out its local campaigns against surveillance, in particular on ALPR technology. Freddy and Arti have been at Lucy Parsons Labs which has been working on the explosive growth of ALPRs for over six years. LPLers have been a partners in the nationwide research and organizing against ALPRs all over the country.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: The New Horizons in Quantum and Space

Tags: Middle Easterns & Africans in Cyber Security (MEACS) | Creator Talk/Panel

When: Friday, Aug 7, 15:00 - 15:59 PDT

Where: LVCCW Level 1 Hall 4 1306 (Middle Easterns & Africans in Cyber Security (MEACS) Community) - [Map](#)

Description:

While the industry obsesses over AI security, two frontier domains are quietly creating the next generation of high-demand security careers: post-quantum cryptography and space security. With NIST's PQC standards finalized, federal migration mandates in force, and harvest now, decrypt later attacks already underway, quantum readiness has shifted from research topic to boardroom priority. Meanwhile, exploding satellite constellations, contested orbits, and rising attacks on ground stations and command-and-control systems have made space a critical infrastructure battleground with a severe talent shortage. This talk breaks down the latest technological advances in both domains, the real-world threats driving demand, and the practical skills, certifications, and communities that can launch your career there. You'll leave with a concrete upskilling roadmap and a clear view of why quantum and space are the smartest career bets in security today.

SpeakerBio: Anshu Gupta

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Cloud Village - Friday - 16:10-16:50 PDT

Title: The New Software Supply Chain Nobody is Securing: MCP

Tags: Cloud Village | Creator Talk/Panel

When: Friday, Aug 7, 16:10 - 16:50 PDT

Where: LVCCW Level 3 W313 (Cloud Village Talks) - [Map](#)

Description:



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: The Permanent Threat: Analyzing Aeternum's Blockchain-Based C2 Operations and Communications

Tags: Malware Village | Creator Talk/Panel

When: Saturday, Aug 8, 14:40 - 15:15 PDT

Where: LVCCW Level 1 Hall 2 600 (Malware Village) Talks - [Map](#)

Description:

In recent years, threat actors have been migrating their command-and-control infrastructure from traditional domains and servers to decentralized platforms that are resilient to takedowns. The Polygon blockchain is one such platform, where encrypted and plaintext instructions can be embedded into immutable smart contracts, making them permanently accessible and beyond the reach of law enforcement seizure. Aeternum is a recently discovered botnet that takes full advantage of this shift. Its operators write encrypted C2 commands directly into smart contracts, and infected machines retrieve them via public Remote Procedure Call (RPC) endpoints, eliminating the need for any attacker-controlled server in the command delivery chain.

This one-way, read-only design functions as a dead-drop resolver that cannot be taken offline through conventional means. The botnet's reach extends beyond a single malware family. Multiple samples across different languages and capabilities like loaders, stealers, RATs, and cryptominers have been found querying the same smart contract infrastructure using a shared function selector. Each brings its own execution techniques, from Early Bird APC injection and multi-layer encryption to Telegram-based exfiltration and sandbox evasion routines targeting analyst environments.

By analyzing malware behaviors, network traffic, decrypting the on-chain payloads, and following the operator's digital footprint across multiple platforms, we were able to trace the infrastructure back to a single infrastructure. In this talk, we will walk through the full investigation from initial sample discovery to on-chain decryption and operator attribution and discuss what defenders need to know to detect blockchain-based C2 at the network level.

Speakers: Chris Navarrete, Sai Sathvik Rupp

SpeakerBio: Chris Navarrete, Senior Principal Security Researcher - CDSS Advanced Threat Prevention (ATP) at Palo Alto Networks

Chris Navarrete is a Senior Principal Security Researcher within the Advanced Threat Prevention team at Palo Alto Networks. His work centers on cutting-edge research in cybersecurity, particularly in threat detection and malware analysis. Previously, he served as an adjunct professor of computer science at San Jose State University, teaching Software Security Technologies. He holds a Master of Science in software engineering with a specialization in cybersecurity from San Jose State University. Chris has presented at major industry conferences, including Black Hat Asia, the Computer Antivirus Research Organization (CARO), the Cyber Threat Alliance's Threat Intelligence Practitioners (TIPS) conference, and Black Hat Arsenal, where he introduced and released BLACKPHENIX — a framework designed to automate malware analysis workflows.

SpeakerBio: Sai Sathvik Rupp, Staff Security Researcher at Palo Alto Networks

Sai Sathvik Rupp is a Staff Security Researcher at Palo Alto Networks and a recent M.S. graduate in Information Security from Carnegie Mellon University. He specializes in vulnerability detection and malware analysis, leveraging his expertise to identify, analyze, and mitigate advanced cyber threats.

Hackers.town - Friday - 15:00-15:59 PDT

Title: The Political economy of AI

Tags: Hackers.town | Creator Talk/Panel

When: Friday, Aug 7, 15:00 - 15:59 PDT

Where: LVCCW Level 1 Hall 4 1420 (Hackers.town) - [Map](#)

Description:

SpeakerBio: Janet Vertesi, Officer at Tech Reclaimers

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: The Polymorphic Agent: From Cross Agent Escalation to Just in Time Defense on Azure

Tags: Cloud Village | Creator Talk/Panel

When: Friday, Aug 7, 15:30 - 16:10 PDT

Where: LVCCW Level 3 W313 (Cloud Village Talks) - [Map](#)

Description:

A permission error halts conventional malware. AI agents are being assigned standing cloud IAM permissions and the autonomy to use them, a combination that breaks an assumption every existing control depends on. The agent reasons its way to an escalation path through the cloud provider's own IAM APIs. We call this the polymorphic agent. This talk presents research cross-agent privilege escalation between independent AI agents & defense around it.

The attack begins with a single poisoned tool description, rewritten to read like routine compliance guidance. The agent parses the injected text, reasons about it, and grants itself elevated IAM roles. this showcases how a compromised Agent A modifies the role assignments of a separate Agent B, running a different framework in a separate environment and never issued a malicious instruction, expanding Agent B's authority entirely through authorized IAM calls. This points directly to two risks named in the OWASP MCP Top 10: Privilege Escalation via Scope Creep (MCP02), achieved through Tool Poisoning (MCP03). To test whether this is agent-specific, we ran the attack across three production agents, including LangChain and Claude Code. All three escalated, the pattern is consistent: prompt-layer guardrails are reformable, human approval is socially engineer-able, and telemetry arrives too late.

These results frame two requirements for any workable defense: the escalation must be measurable in real time, and it must be blocked at a point the agent cannot reach. Enforcement has to move to the credential layer, since an agent cannot act on the cloud without first obtaining a credential. This is the gap PrivilegeGuard closes, an out-of-process credential gateway that intercepts DefaultAzureCredential and slots into existing agent deployments with minimal to no code change.

On each token request, it computes the requesting Non-Human Identity's Blast Radius Score (BRS): the fraction of the cloud resource surface reachable by that identity across a two-hop IAM graph traversal, providers reachable under current role assignments plus those reachable after a simulated roleAssignments/write self-escalation. PrivilegeGuard evaluates BRS and its rate of change against an Open Policy Agent (Rego) policy and denies an anomalous, high-blast-radius request before the escalated role is usable.

The takeaway is architectural: cross-agent escalation follows from giving probabilistic, goal-driven agents standing IAM credentials, not from any single agent or framework, and it widens as agents gain access. We deliver the attack on real Azure identities, and an enforcement model that stops it where the agent cannot follow: the credential layer.

SpeakerBio: Muskan Tomar

Hey, I am Muskan Tomar, a Security and Reliability Engineer at MICROSOFT, where I work at the intersection of Site reliability, Infrastructure Security, and Software Engineering building systems that are expected to never go down, stay secure, and scale quietly in the background. 5X Microsoft Azure Certified , with experience working on architecting and modernising, securing cloud platforms and reducing operational toil through automation, AI and data driven engineering. My independent research focuses on AI agent security and cloud identity, and how autonomous agents change the threat model for systems we trust to stay locked down. An enthusiastic learner who champions collaborative cloud and security research, I enjoy untangling complex systems and eliminating single points of failure. Outside work, I love to travel and paint.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: The Protocol-Native Adversary: Full-Spectrum ICS Simulation via SiL

Tags: Red Team Village | Misc

When: Saturday, Aug 8, 12:00 - 12:59 PDT

Where: LVCCW Level 1 Hall 1 309 (Red Team Village) Workshop Stage 2 - [Map](#)

Description:

As adversaries increasingly target the "physics" of critical infrastructure, the security community must move beyond IT-centric red teaming. While hardware-based training platforms have paved the way, they often lack the scale required to simulate complex, multi-facility sabotage. This workshop introduces a Software-in-the-Loop (SiL) environment designed to bridge the gap between IT command-and-control and OT process logic. Participants will navigate a containerized industrial ecosystem, mastering "Living-off-the-Ladder" (LotL) techniques—using native, unauthenticated protocols (Modbus, DNP3, S7comm) to manipulate physical water treatment processes. We will move through the full ICS kill-chain, focusing on the technical mechanics of memory-block interrogation and automated setpoint manipulation. Attendees will engage in a hands-on lab, executing a "Credential Harvest" (T0861) and a coordinated chemical-override attack. By the end of the session, participants will understand why these "authorized" protocol commands bypass traditional NIDS and will leave with a deployable SiL framework to continue their own ICS research.

Speakers: Blessen Thomas, Javier Hernández, Wojciech Poparda

SpeakerBio: Blessen Thomas

Blessen Thomas is an Independent Security Researcher. He has more than 13+ years of experience in Red Teaming, Appsec (Web, Thick, API & Mobile Apps), Smart Watch Wearable Application Penetration Testing, Mobile Penetration Test (iOS, Android, Windows platform), IoT, OT, mainframes, SAP, SWIFT, RPA, Cloud, ATM, KIOSK, Vulnerability Assessment and Network Penetration Test, Physical Covert Entry, Wireless assessments, Telecom (2G, 3G, USSD) etc. for several enterprise companies and financial institutions all across the globe. He is a B.Tech in Information Technology from Anna University and holds industry certifications such as SANS GPEN, CRTO, OPST, CREST CRT(PEN), CREST CPSA, OSCP, CRTP, OSWP, C)PTE, CEH, CHFI. He has been listed and acknowledged in various "HALL OF FAMES" for various companies such as Oracle, Sony, Kayako, Appcelerator, Hotgloo, Meldium, Splunk and many more for responsible disclosure. He has been a bug bounty hunter and contributor for the OWASP Mobile Testing Guide Project (MSTG), Tamer OS, Seclists, OWASP top 10 API, OSSTMM, Awesome Mainframe Hacking, RvR, WAVSEP Benchmark sectool projects. His research training/talks has been accepted into various security conferences like Hack in the Box-Dubai, Hacktivity -Hungary, CanSecWest -Canada, OWASP Appsec EU- London -UK, OWASP Appsec Europe-Italy, RootCon-Philippines, OWASP PH, OWASP New Zealand Day, Infosec SouthWest, Austin, Texas, FSec-Croatia, Hackbeach, Hackfest, Shakacon, ITWeb-South Africa, Jordan Cyber Security Summit, HITCON-Taiwan, OWASP AppSec-Bucharest, OWASP Appsec Africa-Morocco, CircleCityCon, OWASP Botswana, CactusCon, Bsides-London, Prishtina, Aarhus, Vilnius, Elbsides, Kristiansand, Athens and many more. He has been invited as Speaker for Radio Talk Shows for All India Radio. He spends his leisure time playing drumkit and percussion.

SpeakerBio: Javier Hernández

Javier is a Red Team Operator and Malware Developer specializing in offensive engineering, adversary emulation, and custom tooling development. Holding certifications such as OSEP and CRTO, he has delivered high impact security engagements across both consulting environments and in house security teams. His work focuses on crafting stealthy implants, evasion techniques, and automation driven offensive capabilities. Passionate about applied research, he explores the intersection of malware development and AI augmented offensive security to help organizations strengthen their resilience against modern threats

SpeakerBio: Wojciech Poparda

Wojciech Poparda is a cybersecurity consultant. He helps organizations proactively defend their digital infrastructure by thinking like an adversary. Leveraging a deep foundation in Offensive Security, he specializes in designing resilient Security Architectures that bridge the gap between complex attack vectors and enterprise defense, with a sharp focus on Cloud Security and Identity & Access Management (IAM).

His approach is backed by rigorous technical validation, holding industry-leading certifications including OSCP, CRTE, CRTP, CRT0, CPTS, CWES, AWS Certified Solutions Architect - Associate and AWS Certified Security - Specialty. He is also an Associate of ISC2, having successfully passed the CISSP exam.

Beyond the terminal, he channels the discipline, focus, and resilience required for cybersecurity into his life as a triathlete. As an IRONMAN European and World Championships finisher, he brings the same endurance and dedication to solving complex security challenges as he does to the race course.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: The Quantum Mechanic: Attacking all the clouds

Tags: Red Team Village | Misc

When: Saturday, Aug 8, 16:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 309 (Red Team Village) Tactic Table 1 - [Map](#)

Description:

Cloud environments are now expansive and interconnected, where identity is the main security boundary, and misconfigurations pose security risks. For Red Teamers, attacking these environments often means relying on a collection of mismatched tools. You need one set of scripts for Entra ID, a separate framework for AWS, and many command-line tools for other cloud providers. This switching between tools is inefficient, and workflows require many manual commands. When operators deal with complex dependencies and syntax differences between providers, they miss broader attack paths.

Enter the Quantum Mechanic.

This session introduces a new Unified Cloud Attack tool designed to remove the operational friction of multi-cloud engagements. Built for operators who need to move fast and remain unnoticed, Quantum Mechanic serves as a universal discovery and exploitation engine. It hides the differing command sets of various cloud providers, allowing operators to run complex attacks through a single, consistent interface without sacrificing the accuracy of direct CLI commands.

During this talk, we will discuss the realities of modern cross-cloud exploitation and demonstrate how to bring order to the process. We will present the framework's main components, demonstrating how it handles compromised credentials, automates cross-platform enumeration, and maps privilege-escalation paths. Through demonstrations, we will show the tool's ability to exploit multi-cloud environments with a single command set.

If you are tired of managing multiple separate tools just to get started, or if you've ever disrupted an operation because of a misconfigured cloud script, it's time to upgrade your toolkit. Join us to learn how to streamline your cloud attack workflows and improve precision.

SpeakerBio: Moses Frost

Moses Frost has been working in the field since the late 90's. Working with computers in the late 80s for fun and moving into a more professional field shortly after high school. He is a Red Team Operator at Neuvik. A senior instructor and course author at the SANS Institute, authoring and teaching the Cloud Penetration Testing Course. He also co-authors the book Gray Hat Hacking: Volume 6. He has worked at many companies, notably Cisco Systems, McAfee, and TLO. Currently, he is a Senior Operator at Neuvik. Over those years, he has enjoyed working in all parts of the IT Industry and hopes to do so for many more years.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Voting Village - Saturday - 17:30-17:59 PDT

Title: The Republic is a Team Sport: Technology can Protect Elections, but the People must Protect Democracy

Tags: Voting Village | Creator Interactive Talk/Panel

When: Saturday, Aug 8, 17:30 - 17:59 PDT

Where: LVCCW Level 2 W220 (Voting Village) (Voting Village Talks) - [Map](#)

Description:

Throughout the Voting Village, speakers and researchers have always challenged assumptions around election technology, internet voting, audits, legal frameworks, and the public confidence. Among the many lessons learned together, we can see these issues pointing to a common conclusion that democracy cannot depend on trust alone. But the evidence we develop from security research and academia, are not enough to move our nation in the right direction either.

This closing discussion asks what comes after the research. How do technical findings become better policy? What responsibilities do election officials, attorneys, journalists, academics, and citizens share in preserving institutions that none of us can protect alone? What does it mean to be an American today? This session invites the audience to help answer those questions. Drawing from conversations throughout the conference, we'll explore how democratic resilience depends not only on secure systems, but on communities willing to engage honestly across disciplines and political perspectives.

The goal is not consensus. The goal is responsibility.

SpeakerBio: Kendall Spencer

Kendall Spencer is an attorney specializing in emerging companies, technology transactions, and the legal issues shaping innovation. Since joining DEF CON's Voting Village as a Georgetown Law student in 2019, he has worked alongside Matt Blaze, David Jefferson, and the Voting Village team at the intersection of election technology, cybersecurity, and democracy. Spencer serves on the Board of Directors of the Election Integrity Foundation and has advised state election officials on election security, post-election audits, and cybersecurity best practices. His work focuses on bridging the gap between technical research, public policy, and the law—helping policymakers, election officials, security researchers, and the public better understand the role election security plays in strengthening democratic institutions and public confidence in elections. A frequent DEF CON speaker, Spencer is passionate about fostering thoughtful, bipartisan conversations on the role of technology in protecting election integrity and the democratic principles that underpin a free and open society. Outside of his legal and technology work, Spencer is a rare book dealer and collector specializing in early American history and the Black diaspora.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Bug Bounty Village - Friday - 11:00-11:30 PDT

Title: The Ripple Effect: Inside Cloud-Scale Vulnerabilities in the Age of AI

Tags: Bug Bounty Village | Creator Talk/Panel

When: Friday, Aug 7, 11:00 - 11:30 PDT

Where: LVCCW Level 1 Hall 3 1102 (Creator Stage 6) - [Map](#)

Description:

Security researchers never see the true impact of their work. You submit a vulnerability report, it disappears into a queue, and eventually get a "resolved." But what actually happened on the other side? This talk changes that. Through a real-world case study, you'll see what happens when a single vulnerability report hits a cloud provider at scale and keeps going. What makes cloud vulnerabilities fundamentally different from traditional targets? How do you prioritize remediation when the blast radius spans services, regions, and third-party dependencies you didn't know existed? You'll see the crucial trade-offs no one talks about publicly, and a series of challenges that textbook CVD (coordinated vulnerability disclosure) was never designed to handle. And that challenge is accelerating. AI vulnerability discovery tools are uncovering valid vulnerabilities faster than traditional VDP (Vulnerability Disclosure Program) models were architected to process. The model that worked five years ago is buckling, and its impact is felt across organizations worldwide. Researchers wait longer. Defenders fall behind. The gap between discovery and remediation is widening, and attackers live in that gap. This talk introduces the 3 Principles for modern VDPs, which were forged from operating vulnerability disclosure at the world's largest cloud infrastructure. These apply whether you're running a program or reporting to one. Security researchers will learn what actually happens after you hit submit, and how to write reports that accelerate everything downstream. Defenders will learn how to scale their programs for the velocity that's already here.

Speakers: Albin Vattakattu, Ryan Nolette

SpeakerBio: Albin Vattakattu

Albin leads the global Vulnerability Disclosure Program (VDP) for Amazon Web Services (AWS). Albin's work has been featured by HackerOne, the SANS Institute, the AWS Security Blog, and at multiple international conferences.

Prior to AWS, Albin led incident response teams across North and South America, defending foreign governments and fortune 100 companies against DDoS campaigns by APTs.

SpeakerBio: Ryan Nolette

Ryan is AWS's Senior Security Engineer and CoAuthor of AWS Detective. He has previously held a variety of roles including threat research, incident response consulting, and every level of security operations. With almost 2 decades in the infosec field, Ryan has been on the development and operations side of companies such as Postman, Sqr1, Carbon Black, Crossbeam Systems, SecureWorks and Fidelity Investments. Ryan has been an active speaker and writer on threat hunting and endpoint security.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: The Sandbox is a Suggestion: Deconstructing AI Agent Sandboxes

Tags: DEF CON Official Talk | Demo | Exploit

When: Friday, Aug 7, 16:00 - 16:59 PDT

Where: LVCCW Level 1 Hall 3 1006 (Main Track 1) - [Map](#)

Description:

Every major AI coding agent ships inside a containment system. I analyzed three of them - Anthropic's Claude Code, Google's Gemini CLI, and OpenAI's Codex CLI - and each one breaks on its own terms.

Each sandbox uses a different containment model: permission-based access control, process-level environment sanitization, and kernel-level filesystem enforcement. Each makes a structural assumption about what the runtime will do. Each assumption is wrong.

This talk deconstructs all three architectures, shows what each claims to enforce, and demonstrates how the containment fails - not through prompt injection or model persuasion, but through gaps in the design itself. Every exploit is deterministic, demo-ready, and was reported through coordinated disclosure.

Attendees leave with a reusable methodology for evaluating any AI agent sandbox: identify the containment mechanism, read the enforcement code, find the structural assumption it depends on, and test whether the runtime violates it. The cross-vendor comparison shows that different engineering teams, solving the same problem independently, make structurally similar mistakes - and that the pattern is predictable once you know where to look.

SpeakerBio: Elad Meged, Novee Security

Elad Meged is a Founding Engineer and Security Researcher at Novee Security, specializing in offensive security research and AI security. He holds an M.Sc. in Computer Science and has a background in vulnerability research across web, mobile, and low-level systems, with experience in reverse engineering and platform internals. His current work applies offensive research methodology to AI systems while developing AI-driven approaches to vulnerability discovery and exploit verification.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: The Sherlock Holmes Social Engineering Playbook

Tags: Social Engineering Community Village | Creator Talk/Panel

When: Saturday, Aug 8, 14:30 - 14:59 PDT

Where: LVCCW Level 3 W317-319 (Social Engineering Community Village) - [Map](#)

Description:

Long before phishing, deepfakes, and business email compromise, Sherlock Holmes was demonstrating social engineering tactics: building trust, gathering intel, exploiting emotion, and manipulating human behavior to achieve an objective. The tools have changed. The psychology has not. In The Sherlock Holmes Social Engineering Playbook, we examine how Sir Arthur Conan Doyle's detective stories function as a masterclass in human hacking. Through cases such as A Scandal in Bohemia, The Red-Headed League, and The Sign of Four, this presentation breaks down techniques used to influence decisions, lower defenses, and extract information, many of which mirror modern phishing, OSINT, and fraud campaigns. Through immersive examples and practical cyber parallels, attendees will explore how Holmes used recon, pretexting, impersonation, trust-building, distraction, and emotional leverage to accomplish his goals, and how attackers rely on those tactics today. Participants will leave with a practical social engineering playbook for recognizing manipulation, strengthening human defenses, and thinking critically about the psychology behind cyber threats. Because sometimes the best way to understand today's attackers' is to study a Victorian detective.

SpeakerBio: Elizabeth Rasnick, Assistant Professor at Center for Cybersecurity and Artificial Intelligence at the University of West Florida

Dr. Elizabeth Rasnick is an Assistant Professor at the Center for Cybersecurity and Artificial Intelligence at the University of West Florida. Her work focuses on human-centered cybersecurity, workforce development, cybersecurity education, and the intersection of psychology, storytelling, and social engineering. Dr. Rasnick specializes in translating complex cybersecurity concepts into engaging, accessible learning experiences for technical and non-technical audiences alike. Her research and presentations explore how human behavior, persuasion, trust, and cognitive bias shape modern cyber threats, often through unexpected lenses such as literature, history, and pop culture. She is particularly interested in how classic narratives, including Sherlock Holmes, reveal timeless social engineering tactics still used by attackers today. A frequent speaker, educator, and advocate for interdisciplinary cybersecurity education, Dr. Rasnick works to broaden participation in cybersecurity and prepare the next generation of cyber defenders through innovative, experiential learning. Whether discussing phishing, persuasion, OSINT, or the psychology of manipulation, she believes the most effective security begins with understanding people.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: The Silent Tunneler: A Real-World Incident Response Story

Tags: Malware Village | Creator Workshop

When: Friday, Aug 7, 10:10 - 11:40 PDT

Where: LVCCW Level 1 Hall 2 600 (Malware Village) Workshops - [Map](#)

Description:

Some backdoors are noisy. Others whisper.

During a real-world Incident Response investigation, I uncovered an unusually stealthy Linux persistence mechanism that had silently granted an attacker continued access to a compromised system. Even more concerning - it was used to establish an SSH tunnel, allowing undetected remote control while evading traditional security measures.

But that wasn't all. Further analysis led to an even bigger discovery: a live Mirai botnet infection, actively communicating with its command-and-control server. By reverse engineering the malware, I unraveled how it spread, operated, and executed attacks.

This talk is a practical, real-world case study, covering: * How I uncovered an unconventional backdoor that nearly went unnoticed. * The attacker's use of SSH tunneling for covert persistence. * Reverse engineering a Mirai botnet sample and dissecting its attack mechanisms. * Key lessons for defenders to detect and respond to stealthy threats.

Expect live demonstrations, technical deep dives, and actionable insights to strengthen your EDR detection capabilities.

SpeakerBio: Uriel Kosayev, Security Researcher, Trainer & Speaker | Author of the Antivirus Bypass Techniques book | Founder of TrainSec Academy

Uriel Kosayev is a seasoned cybersecurity researcher, reverse engineer, and keynote speaker with over a decade of hands-on experience in malware analysis, offensive security, and real-world incident response.

He is the founder of TrainSec Academy and the author of Antivirus Bypass Techniques and MAoS – Malware Analysis on Steroids, two highly regarded resources in the cybersecurity community. Uriel has worked with global enterprises, led red team operations, and conducted high-impact malware investigations that exposed advanced threat actor tactics.

Known for his ability to break down complex topics into practical, actionable knowledge, Uriel teaches with one goal in mind: to make professionals think like attackers and act like defenders. His courses are packed with real-world examples, battle-tested techniques, and a methodology built on actual field experience, not textbook theory.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Malware Village - Friday - 14:55-15:35 PDT

Title: The State of Decompiler Malware

Tags: Malware Village | Creator Talk/Panel

When: Friday, Aug 7, 14:55 - 15:35 PDT

Where: LVCCW Level 1 Hall 2 600 (Malware Village) Talks - [Map](#)

Description:

This research introduces Decompiler Malware, an underexplored threat category targeting reverse engineering platforms such as IDA Pro. The work began with the discovery and analysis of a malicious IDA Pro plugin that established a covert encrypted backdoor capable of remotely interacting with the analyst environment, manipulating analysis workflows, and exfiltrating decompiled pseudocode and reverse engineering artifacts on demand.

By examining the malware's architecture, command capabilities, and operational design, this research highlights how reverse engineering workstations represent a uniquely valuable but insufficiently defended attack surface (unless air-gapped).

SpeakerBio: Christopher Hernandez, Binary Enthusiast

Chris Hernandez is a security researcher specializing in vulnerability discovery, exploitation, and large scale reverse engineering using IDA Pro. A Pwn2Own competitor in the ICS/SCADA and embedded systems categories, he actively collaborates with the reverse engineering community to solve binary analysis challenges.

--

Chris Hernandez is the founder of Adversary Consulting Group and an offensive security researcher with more than a decade of experience in vulnerability research, reverse engineering, and exploit development. He holds the OSEE certification and has competed at Pwn2Own in the IoT and ICS/SCADA categories.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

DEF CON Groups - Sunday - 11:00-11:30 PDT

Title: The State of DEF CON Groups

Tags: DEF CON Groups | Creator Talk/Panel

When: Sunday, Aug 9, 11:00 - 11:30 PDT

Where: LVCCW Level 1 Hall 3 1100 (Creator Stage 7) - [Map](#)

Description:

DEF CON Groups has grown into a global network of hundreds of local communities, connecting hackers, makers, students, educators, and professionals around the world. Join the department leadership for an inside look at where the community stands today, what we've accomplished over the past year, and where we're headed next.

We'll share highlights from across the global DEF CON Groups community, new initiatives, lessons learned, available resources for Group organizers, and ways anyone can get involved—whether you're looking to attend your first local meetup, volunteer, help organize an existing Group, or start one in your own city.

Whether you're a longtime Group organizer or just discovering DEF CON Groups, this session is your opportunity to hear directly from the department, celebrate the community's achievements, and see what's coming next.

Speakers: Alethe Denis, Magen Wu

SpeakerBio: Alethe Denis, DCG, Lead Goon

No BIO available

SpeakerBio: Magen Wu, Director of Ops Goon at DEF CON Groups

No BIO available

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: The Stream Is Dead, Long Live the Stream: How HTTP/2 Lets Dead Streams Keep Servers Working

Tags: DEF CON Official Talk | Demo | Tool | Exploit

When: Friday, Aug 7, 15:00 - 15:59 PDT

Where: LVCCW Level 1 Hall 3 1006 (Main Track 1) - [Map](#)

Description:

Modern protocol bugs rarely look like flaws in the protocol itself. They show up when a clean spec meets existing server architectures. HTTP request smuggling showed this for request boundaries: implementations disagreed about where one request ended and the next began. This talk asks a similar question about HTTP/2 request lifetime: what happens when one layer thinks a request is over, while another is still working on it?

In 2023, Rapid Reset showed the world that HTTP/2 had a problem: attackers could open and reset streams faster than servers could keep up. The disclosure triggered an industry-wide patching scramble, but patches addressed the symptom, not the root cause.

Two years later, I disclosed MadeYouReset through CERT/CC as CVE-2025-8671, exploiting the same root cause through a different door and setting off a second round of patches across the ecosystem, including Apache Tomcat, H2O, Netty, and others.

In this talk, I'll show how research that started with Rapid Reset led to MadeYouReset, and how both create streams closed at the HTTP/2 layer while server-side request work continues. We'll see why this gap exists, why fully fixing it is infeasible, and what conditions make MadeYouReset especially harmful.

Finally, we'll answer the question: is the next HTTP/2 abuse already waiting around the corner?

CERT/CC VU#767506: <https://kb.cert.org/vuls/id/767506> NVD CVE-2025-8671:

<https://nvd.nist.gov/vuln/detail/CVE-2025-8671> MadeYouReset blog posts: <https://galbarnahum.com/made-you-reset>

SpeakerBio: Gal Bar Nahum, Tenzai

Gal Bar Nahum is a security researcher at Tenzai with eight years of experience in vulnerability research, network protocol security, red teaming, and AI research.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: The Subverted Hacker

Tags: Policy @ DEF CON | Creator Talk/Panel

When: Saturday, Aug 8, 13:30 - 13:59 PDT

Where: LVCCW Level 1 Hall 3 801 (Creator Stage 1) - [Map](#)

Description:

Frontier AI is turning hacker labor into a defensive layer for private infrastructure: systems built on public research, open-source code, security writing, and the technical culture hackers helped create. Yet these systems are controlled by a small number of companies and states, with limited public audit ability or accountability. Historically, hackers made complex systems more understandable, modifiable, and contestable. In frontier AI, that role is being subverted. Hackers are recruited (or bribed viabounties ha!) to harden opaque models, reduce adversarial access, and protect systems whose impacts are public, but whose internals, evaluations, and risk decisions remain private. Public-interest scrutiny remains in conflict of interest. This talk argues that AI security cannot become only a corporate risk or national competitiveness exercise. If frontier AI affects labor, speech, art, security, and institutions across the globe, then it needs international public-interest security obligations. I propose an international AI evaluation and red-team mandate: a legally protected mechanism that brings vetted hackers and experts from across the globe into controlled testing of high-impact AI systems, so they remain contestable and accountable beyond the companies that build them. (I can dream can't I?)

SpeakerBio: Robert "zizkill" Shala, Sentry

Robert Shala is co-founder of Sentry, a company delivering security assurance services for some of the world's largest organizations. His work sits at the intersection of offensive security, public policy, and emerging technology governance. Robert has contributed to Kosovo's national cybersecurity strategy working group and to a Kosovo working group on responsible AI use in military contexts. He is also the founder of DEF CON Group Prishtina, where he works on advancing Kosovo's responsible disclosure ecosystem and improving legal protections for good-faith security research. He has served as an external AI Red Teamer for OpenAI, probing frontier models for safety and security flaws, and was formerly involved with Georgetown RAIN/GAIA. Robert has presented security research at the Defence Academy of the UK, DEF CON 33 at AI Village and AppSec Village, and BSides across the world. He holds an M.A. in Security Studies from Georgetown University and a B.S. from RIT. Robert loves wargaming.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Social Gatherings/Events - Wednesday - 11:00-17:15 PDT

Title: The Unofficial DEF CON Shoot

Tags: Event

When: Wednesday, Aug 5, 11:00 - 17:15 PDT

Where: Other / See Description

Description:

The Unofficial DEF CON Shoot is a public event that happens just prior to the DEF CON hacker conference in Las Vegas, Nevada. It is an opportunity to see and shoot some of the guns belonging to your friends while taking pride in showing and firing your own steel, as well, in a relaxed and welcoming atmosphere. We choose a spot, then we rent tables, canopies, and bring all the necessary safety equipment and amenities. All you need to bring yourself and (optionally) your firearms. New shooters and veterans both attend regularly. You can attend with your firearms, of course, but folk without guns of their own in Vegas may have the opportunity to try gear from others in attendance.

Pro Gun Vegas - 12801 Old US 95 Boulder City, NV 89005

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Blacks In Cyber Village - Saturday - 12:30-12:55 PDT

Title: The Voice Behind the Payload: Tracing AAVE Across Malware Artifacts

Tags: Blacks In Cyber Village | Creator Talk/Panel

When: Saturday, Aug 8, 12:30 - 12:55 PDT

Where: LVCCW Level 3 W322-W324 (BIC Village) - [Map](#)

Description:

Discover an often-overlooked signal in threat actor attribution: everyday language. This compelling session explores how African American Vernacular English (AAVE), with its distinctive grammatical features and lexicon, can leave unique fingerprints in malware artifacts like ransom notes and phishing lures. While emphasizing that AAVE use doesn't imply threat actor ethnicity, this talk will dive into a YARA-based detection methodology to investigate its frequency across malware samples. Attendees will learn about the study's innovative approach, review preliminary findings on which malware families show the strongest signals, and engage in crucial discussions around the ethical implications of sociolinguistic analysis in cybersecurity. Don't miss this fascinating look at how linguistics can enhance our understanding of threat actor intent and capabilities.

SpeakerBio: Brett Alexander Tolbert, Principal Cyber Threat Intelligence Analyst / Undergraduate Adjunct Professor at Bowie State University

Brett Tolbert is a Principal Cyber Threat Intelligence Analyst and an undergraduate adjunct professor at Bowie State University. With over 11 years of experience in cybersecurity, they have held threat intelligence and cyber defense roles in the U.S. intelligence community and in companies supporting U.S. critical infrastructure, focusing on tracking Asia-nexus state-sponsored threat actors, threat intelligence engineering, cross-sector partnerships, and technical leadership. They have previously spoken at SANS CTI Summit, MITRE ATT&CKcon, and the BIC Village at DEFCON. Brett lives in the DC-Baltimore corridor and enjoys playing monster hunter games, knitting, and baking in their spare time.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: There and Back Again

Tags: Voting Village | Creator Talk/Panel

When: Friday, Aug 7, 15:30 - 15:59 PDT

Where: LVCCW Level 2 W220 (Voting Village) (Voting Village Talks) - [Map](#)

Description:

In 2025, Mojave Research received an assignment its founders never expected: examine security vulnerabilities in voting equipment used during Puerto Rico's 2024 elections. What appeared to be a bounded technical project quickly became a journey through voting technology, digital forensics, incomplete evidence, institutional friction, and the difficult line between what a system could permit and what the evidence proves actually happened. Jason Wareham and Manbir Gulati will explain how Mojave became involved, what the team was asked to do, and how two outsiders to election administration found themselves examining technology at the center of a national argument about security and public trust. Jason will describe the origins and evolution of the assignment, along with the challenge of keeping a technical investigation tied to evidence when others already have firm expectations about the answer. Manbir will take the audience inside the technical problem at a level appropriate for public discussion: how investigators approach unfamiliar election systems, assess available hardware and software, reason from constrained artifacts, evaluate weaknesses, and separate a possible attack path from evidence of exploitation and what remains to ensure the security of these critical systems is inviolate. Mojave's examination identified real software and security concerns. It did not YET find evidence that the equipment examined had been hacked or that votes had been altered. That distinction is central to the story—and to any honest discussion of election security. The talk will conclude with an announcement of, and invitation to, a private initiative aimed at reducing voting-system risk before the 2026 midterm elections absent of politics. This is a brief account of how a national-security startup entered an unfamiliar and politically charged field, followed the evidence through an unexpected assignment, and concluded that documenting the problem was not enough.

Speakers: Jason Wareham, Manbir Gulati

SpeakerBio: Jason Wareham

Jason Wareham is CEO of Mojave Research Inc. and CEO and Chairman of Agentic Secure Group. In 2025, the Office of the Director of National Intelligence (ODNI) engaged Mojave Research to examine security vulnerabilities in voting equipment used during Puerto Rico's 2024 elections.

Jason previously spent nearly two decades handling military, criminal-defense, and national-security matters. He served as a U.S. Marine Corps officer and judge advocate and reached the rank of lieutenant colonel. His work included trials, appeals, military commissions at GTMO, classified information, and digital evidence. The Marine Corps designated him a Master of Criminal Law, and he later worked as a senior litigation adviser and trainer before concluding his private practice.

Jason holds an LL.M. from Georgetown University Law Center, where his studies focused on cybersecurity, digital forensics, electronic discovery, and cybercrime. He earned his J.D. from Creighton University and authored "Cracking the Code," a Georgetown Law Technology Review article about compulsory decryption and the Fifth Amendment.

At Mojave Research, Jason works on national-security technology, secure artificial intelligence, cybersecurity, and technical investigations subject to legal and institutional scrutiny. His approach is simple: establish what the evidence proves, identify what it does not prove, and resist pressure to blur the difference.

SpeakerBio: Manbir Gulati

No BIO available



Title: There Is No Internet: Cross-Domain Recon of all 4.3 Billion IPv4s

Tags: Recon Village | Creator Talk/Panel

When: Saturday, Aug 8, 17:30 - 17:59 PDT

Where: LVCCW Level 1 Hall 3 801 (Creator Stage 2) - [Map](#)

Description:

We scanned every IPv4 address on the planet. Twice. We collected public records in one of at least three places: the RIR registration, the operator's reverse DNS, or whatever service answers on port. Most threat intelligence pipelines read one of those. Darkmouse lines up all of them and flags the disagreements. The result is attack-surface visibility that no single source gives you, and a methodology you can run yourself.

This talk walks the recon pipeline behind three findings from a single cross-domain pass over 4.3 billion IPv4 addresses in five days, plus a 92 million IP targeted scan in 34 hours (Russia, Iran, and North Korea). We used ZMap on single-use Jetstream2 VMs, zdns for PTR and forward verification, bulk RPSL and ARIN XML and APNIC data loaded into DuckDB alongside MaxMind GeoLite2, OpenSanctions, and the US Trade Consolidated Screening List. Enrichment is baked into the scan row at ingest. Every field carries a source-date stamp so longitudinal comparison actually works.

Lead finding for a recon audience: 6,656 Iranian IPs in RIPE where the registrant placed fabricated US street addresses into the authoritative registry. 4,608 of them cite AT&T Mobility's ARIN IP-management address verbatim. 2,048 cite a Philadelphia apartment building. All geolocate to Iran. All trace to one operator through a shared RIPE maintainer object linking a Shiraz Local Internet Registry and an Omani shell.

Between September 2025 and January 2026 the fabricated addresses began rotating out, replaced by netnames like "Datacamp-Limited" that impersonate real UK hosting companies. A single-point-in-time feed cannot see that rotation. Two dated snapshots can. We are currently running follow up scans and expect to have new data before the conference.

Additional Findings: five active PTR records in Russia and the Netherlands claiming US government domains, including .fbi.gov subdomains, four of five still live six months after first observation (April 2026). And 1,534 APNIC-registered IPs for Entity Listed Chinese telecoms, declared country=US, geolocating to One Wilshire in Los Angeles, running production email and DNS on FCC-revoked Section 214 infrastructure.

Every finding ships with the RDAP query, the DNS check, and the cross-reference that verifies it. Every finding ships with the RDAP query, the DNS check, and the cross-reference that verifies it. Attendees leave knowing which four sources to line up, which fields to trust, and what to look for when two dated snapshots disagree.

SpeakerBio: John McCary, Former DARPA, State Department, now Professor and Builder

John McCary founded Port 194 LLC, where he builds internet-scale measurement and correlation tooling from public data. Former soldier, diplomat, Wall Street Journal journalist, licensed private investigator, and certified ethical hacker. At 29 he helped design and launch a peer-to-peer data sharing platform that became a DARPA program of record and is still in use today. He designed and teaches the Open Source Intelligence course at the University of Arizona as adjunct faculty. Off the clock he is usually underwater, in a Muay Thai gym, or playing live music, though rarely at the same time.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: There's A Bug in My Boot! Finding Vulnerabilities in U-Boot

Tags: Packet Hacking Village | Creator Talk/Panel

When: Saturday, Aug 8, 15:00 - 15:59 PDT

Where: LVCCW Level 1 Hall 3 1102 (Creator Stage 6) - [Map](#)

Description:

Bootloaders underpin the security of modern embedded systems. Their privileged position in the tech stack often means a vulnerability early in the boot process can result in total system compromise. Despite this, they frequently lack modern software security protections (ASLR, CFI, Stack Canaries), making them an easier target to exploit. This talk will explore hardware-in-the-loop, emulation, and native binary fuzzing approaches with U-Boot, a popular embedded system bootloader for networking devices, and the challenges each approach presents.

SpeakerBio: Jared Stroud, Lead Reverse Engineer, The Johns Hopkins University Applied Physics Lab

Jared Stroud is a Lead Reverse Engineer at The Johns Hopkins University Applied Physics Lab. Currently he's pursuing a Doctorate of Engineering focused on scaling vulnerability identification and remediation in embedded systems. For the past 7 years Jared has documented independent security research at Arch Cloud Labs (<https://www.archcloudlabs.com/projects>), and has presented workshops on reverse engineering topics at DEF CON, Shmoocon, and BSides Rochester.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Thin Client? Thin Crypto - Bypassing Full-Disk Encryption Across Three Major Thin Clients Vendors without Breaking a Cipher

Tags: DEF CON Official Talk | Demo | Exploit

When: Saturday, Aug 8, 11:30 - 12:30 PDT

Where: LVCCW Level 1 Hall 3 1007 (Main Track 2) - [Map](#)

Description:

Thin clients are deployed across healthcare, finance, government and critical infrastructure, environments where full disk encryption is a compliance requirement, not optional. Dell, IGEL and HP all ship FDE backed by TPM hardware and modern cryptography. I broke all three.

I present new research demonstrating vulnerabilities that permit full disk encryption bypass across Dell ThinOS 9.x - 10.x, HP ThinPro 8.x - 9.x, and IGEL OS 11.x - 12.x. Every attack achieving filesystem access from a powered-off device with no credentials and no specialist hardware. Behind the encryption: WiFi credentials, 802.1x NAC client certificates, VDI session configs, management server credentials, and password hashes. Compromised devices provide a foothold into the infrastructure it was connected to. I trace Dell's implementation across three generations getting progressively further from best practice, show IGEL's correct PCR policy and modern cryptography bypassed through their own signed bootloader, and demonstrate HP's implementation undone by an unmeasured boot chain.

SpeakerBio: Darren McDonald, AmberWolf

Darren McDonald is an offensive security consultant at AmberWolf, where he specialises in hardware hacking and red teaming. He has spent 17 years breaking into things professionally, starting with networks and applications before moving to embedded systems, firmware, and the physical layer. The kind of hacker who pulls out screwdrivers instead of a checklist.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Radio Frequency Village - Saturday - 13:30-13:55 PDT

Title: This is a Test: Vibe Hacking LTE Cell Broadcast for Emergency Alert Injection

Tags: Radio Frequency Village | Creator Talk/Panel

When: Saturday, Aug 8, 13:30 - 13:55 PDT

Where: LVCCW Level 1 Hall 1 409 (Radio Frequency Village) - [Map](#)

Description:

Every month, billions of mobile subscribers worldwide receive Presidential Alerts, AMBER alerts, earthquake warnings, and severe weather notifications directly to their phones through the 3GPP Public Warning System (PWS). This encompasses CMAS, ETWS, and EU-Alert. These messages bypass all user settings, cannot be blocked, and are trusted implicitly by the public. But what if the tower screaming at your phone isn't a tower at all?

This talk exposes the fragile trust model underlying emergency alerting on modern LTE networks globally. We dissect how PWS messages are transported at the physical and protocol layers, from SIB10/11/12 broadcast blocks down to the exact ASN.1 encoding, and demonstrate how an attacker with modest RF resources can inject, spoof, and manipulate these alerts at scale using software-defined radio.

We'll begin with a technical primer on PWS architecture in LTE, explaining how Cell Broadcast Service (CBS) messages propagate from alert aggregators through carrier core networks to individual eNodeBs, and ultimately to handsets worldwide via the BCCH. Then we shift to the offensive perspective: using a USRP B210 and open-source LTE stacks, we show how to craft malicious SIB messages, impersonate legitimate carrier cells, and force target devices to display arbitrary alert text, including spoofed presidential alerts and hyper-localized fake emergency notifications.

The presentation includes live demonstrations, open-source release of our PWS injection toolkit, and a discussion of responsible disclosure findings shared with carriers and regulators across multiple countries. No prior LTE expertise is required, but familiarity with SDR concepts and cellular architecture will help attendees maximize their takeaways. Attendees will leave understanding exactly why global wireless emergency alerting lacks cryptographic authentication, how trivial the barrier to entry is for alert spoofing.

SpeakerBio: XtraRaj, Mechanic, Car Hacking Village

Ayyappan is a cybersecurity enthusiast interested in hacking and securing everything from wireless, automotive, IoT security, and critical infrastructure. He has published several high-impact CVEs relating to the automotive and IoT sectors and loves to tinker with every electronic device he can get his hands on. Notably, he once successfully turned a doorbell into a botnet that rickrolls visitors.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: This Message Was Sent by Microsoft: Turning Microsoft Apps into our Phishing Platform

Tags: DEF CON Official Talk | Demo | Exploit

When: Sunday, Aug 9, 10:00 - 10:59 PDT

Where: LVCCW Level 1 Hall 3 1007 (Main Track 2) - [Map](#)

Description:

Last DEF CON, we stole cleartext credentials directly from the real Microsoft login page. This year, we take it a step further by making Microsoft deliver our phishing emails!

We've all seen threat actors abuse built-in email notifications from legitimate SaaS platforms to send phishing links from trusted domains, bypassing email security solutions. But in most cases, they only control a small portion of the email content, making the end result far from convincing.

While the execution of these examples has mostly been fairly poor and limited in complexity so far, the idea of making a legitimate application deliver your phishing payload did intrigue me. So I started digging for more advanced ways to push this concept further, looking for techniques that would allow taking over the majority (or sometimes the entirety) of the email content.

In this talk, I'll present several novel techniques to inject custom phishing pretexts into emails sent by multiple first-party Microsoft services, taking advantage of their trusted email addresses and domain reputation.

These emails seem so legitimate that even seasoned IT and security professionals would trust them (and we have the proof from our assessments to back this up). After all, who doesn't trust Microsoft?

- DEFCON33 - Turning Microsoft's Login Page into our Phishing Infrastructure
 - ◆ <https://www.youtube.com/watch?v=z6GJqrkL0S0>
- GraphSpy
 - ◆ <https://github.com/RedByte1337/GraphSpy>
- SharePoint SendEmail API retirement
 - ◆ <https://support.microsoft.com/en-us/office/retirement-of-the-sharepoint-sendemail-api-b35bbab1-7d09-455f-8737->

SpeakerBio: Keanu "RedByte" Nys, Spotit

Keanu Nys (aka RedByte) is an information security researcher from Belgium, and currently leads Spotit's offensive security team. While he has a passion for all offensive cybersecurity topics, he mostly specializes in Active Directory, Microsoft Entra ID (Azure AD), and Social Engineering.

He is the author of the Microsoft 365 and Entra attack toolkit GraphSpy. Additionally, Keanu is the trainer for the Certified Azure Red Team Expert (CARTE) bootcamps at Altered Security, and has given talks, workshops and trainings at conferences like DEF CON, Blackhat USA, and BruCON.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: This Wasn't AI Generated: Principles for Breaking Generative Watermarks

Tags: AI Village | Creator Talk/Panel

When: Saturday, Aug 8, 12:00 - 12:45 PDT

Where: LVCCW Level 1 Hall 3 1103 (Creator Stage 5) - [Map](#)

Description:

The SynthID watermark was developed by Google to invisibly tag content generated by its models and agents (Nano Banana, Gemini, etc.). When asked to identify whether an image is AI-generated, Gemini will invoke a "Verify AI" tool to scan for the SynthID. We demonstrate two attack strategies to remove it. (1) The lesser-known regeneration attack of Zhao et al. 2023 removes SynthID identification by Gemini with 100% success rate on a held-out set of 104 photorealistic Nano-Banana images. (2) We build a surrogate detector using Apple's Pico-Banana-400K dataset. This dataset pairs Flickr images with a Nano-Banana edit, which automatically adds SynthID, thereby implicitly providing us with a large corpus of watermarked/clean image pairs which we use to fine-tune a pre-trained ResNet-18 into a SynthID discriminator. This surrogate detector can be used to test the presence of the watermark in an image in ~27.5 ms on a CPU, thereby allowing an adversary to rapidly test and optimize an attack. We demonstrate that the removal of the SynthID can induce hallucinations, whereby Gemini confidently makes assertions regarding its own simulated as if it were real. This, we propose, could have a variety of security implications, such as confused deputy attacks against agents, retrieval pipeline poisoning, and facial recognition bypasses. The full code, the test set, the pre-computed attack outputs, and the prompts used to generate every test image are released as a hands-on kit at <https://github.com/rabbanitw/WAVES/tree/synthid-regen-kit>

Speakers: Thomas Mason, Tahseen Rabbani

SpeakerBio: Thomas Mason

Thomas Mason has spent the past decade working as a security engineer and offensive pentester. With an original background in machine learning and applied math, he spent several years as a data scientist and OSINT researcher before becoming a pentester in industry. His seven-plus years of pentesting experience gave him a background in a diverse array of offensive security roles, including physical security and social engineering, web, application and network testing, hardware and IoT security, and red teaming. Currently, he works for Coalfire, specializing in cloud and web security with an emphasis on AI products. Outside of his day-to-day work, his research centers on mapping and testing the emerging attack surfaces of large language models, and how their adoption changes the threat landscape. In addition, he works on independent projects combining his background in mathematics and social sciences with his security experience. His hobbies include reading, sports, and graphic novel writing.

SpeakerBio: Tahseen Rabbani

Tahseen is a machine learning Postdoctoral Scholar at the University of Chicago, co-hosted by Ce Zhang and Tian Li, and a Forward Deployed Engineer at Appen. His research focuses on watermarking system efficiency, distributed learning, and privacy. His secondary research interests include numerical optimization and machine translation. His work has appeared at venues such as NeurIPS, ICML, ICLR, and ACL. He received his Ph.D. in Computer Science in 2024 from the University of Maryland, advised by Furong Huang. Prior to the University of Chicago, he worked as a Postdoctoral Associate at Yale, where he worked on low-resource clinical models and fast drug discovery. He obtained his BA in mathematics from the University of Virginia, where he specialized in combinatorial group theory and error-correction, which he continues to work on for fun.

His core research contributions include (1) WAVES, a popular benchmark for stress-testing deep learning-based watermarks under a large suite of attacks; (2) SWIFT, a strategy for asynchronous transmission of model weights over decentralized communication graphs, enabling data-secure collaborative machine learning; (3) Sketch-GNN, a sketch-based compression framework for training graph neural networks with sublinear computational complexity; and (4) PGHash, a novel family of pseudo-random hash functions for private pruning of large classification layer neurons, allowing extreme compression of large

recommender systems.

His work on the WAVES benchmark was spun into the 2024 NeurIPS competition, “Erasing the Invisible,” which drew 2700+ submissions from nearly 250+ global teams, assessing their ability to remove watermarks in black-box and grey-box systems. This competition resulted in many novel attack vectors for effectively destroying nearly every state-of-the-art open-source watermark. He is also a regular reviewer for IEEE Transactions in Multimedia, where he lends his expertise on new watermark designs.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Thread Carefully

Tags: Embedded Systems Village | Creator Event/Activity

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 2 503 (Embedded Systems Village) - [Map](#)

Description:

Presentation about open thread networks, what a thread devices can see from your home network, what can it access. And how this might be mis-used. Some theoretical attack scenarios. Like how to turn a thread only lightbulb with ota update into a residential proxy node.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Threat Actors: Gotta Catch 'Em All

Tags: Recon Village | Creator Workshop

When: Friday, Aug 7, 12:40 - 15:10 PDT

Where: LVCCW Level 1 Hall 2 501 (Recon Village) - [Map](#)

Description:

Your mission: Stop chasing single indicators and start profiling the actual behavior of the adversary. From cybercriminals to state-sponsored actors, every threat group leaves a unique operational blueprint. Whether you are an OSINT hobbyist or an experienced cyber intelligence analyst, come ready to dissect real-world attack behaviors, translate data into actionable insights, and master the art of OSINT-powered TTP research.

This hands-on workshop explores the world of cyber threat actors and the open-source intelligence (OSINT) methodologies used to unmask their behavioral patterns. Rather than focusing strictly on fleeting indicators of compromise (IoCs) like file hashes or IP addresses, participants will learn how to extract, analyze, and profile an adversary's true Tactics, Techniques, and Procedures (TTPs).

Through interactive, real-world case studies, attendees will learn how to analyze public incident reports, open intelligence repositories, and external datasets to map out an actor's operational playbook. Using frameworks like MITRE ATT&CK and the Diamond Model, participants will practice pivoting from technical data to strategic threat profiles—equipping them with the research skills needed to predict and counter adversarial behavior without ever needing an enterprise budget.

Workshop Structure:

Module 1: Foundations of Threat Intelligence & Actor Profiling

The Threat Landscape: Definitions and categories of actors (APTs, cybercriminals, hacktivists, insiders).

Understanding Adversarial Motivation: Moving beyond what happened to why and how actors select their targets and techniques.

Intelligence Categorization: Differentiating between Strategic, Operational, and Tactical/Technical intelligence, and how TTP research feeds all three.

Module 2: The Analytical Frameworks

MITRE ATT&CK Deep Dive: Navigating the matrix, understanding sub-techniques, and avoiding common mapping pitfalls.

The Diamond Model: Connecting the four core nodes (Adversary, Capability, Infrastructure, Victim) to tell a complete campaign story.

The Pyramid of Pain: Understanding why tracking TTPs inflicts the maximum cost on the adversary compared to trivial indicators.

Module 3: Dissecting the Data (Case Study Analysis)

Deconstructing DFIR Reports: Walking through real-world incident examples (e.g., Gootloader campaigns, ransomware operations) to extract behavioral indicators from public write-ups.

Safe Analysis Practices: Utilizing basic web-based OSINT tools (urlscan.io, Browserling, CyberChef) to safely evaluate delivery mechanisms and landing pages without compromising investigator safety.

Module 4: Live TTP Research (Group Exercise)

The Scenario: Groups are given an initial, ambiguous threat brief or a raw dataset from a recent campaign.

The Analysis: Using open-source resources, teams will collaborate to identify the actor's threat components (who, what, where, when, how, why).

The Playbook: Teams will map their findings into the MITRE ATT&CK Navigator, build a comprehensive threat intelligence profile, and present their adversarial playbook to the room.

Speakers: Marcelle Lee, Will Thomas

SpeakerBio: Marcelle Lee

No BIO available

SpeakerBio: Will Thomas

No BIO available

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Threat Hunting 101: Beyond the Alerts

Tags: Blue Team Village | Creator Talk/Panel

When: Saturday, Aug 8, 11:00 - 11:59 PDT

Where: LVCCW Level 2 W217 (Blue Team Village) Main Stage - [Map](#)

Description:

Detection and response are essential pillars of cybersecurity, but what if something slips through the cracks? Not every attack triggers an alert. That's where Threat Hunting comes in.

Threat hunting is a proactive, human-driven approach to uncovering signs of compromise that automated systems may have missed or misunderstood. It involves asking deeper questions, forming hypotheses, and exploring system behavior to find evidence of stealthy or novel attacks.

Join us for an introductory presentation on Threat Hunting, where you'll learn how cybersecurity professionals go beyond known threats to uncover hidden adversaries and why human intuition is still a critical part of modern defense.

SpeakerBio: Kainu ~

With over 18 years of experience in IT and cybersecurity, Kainu currently specializes in Digital Forensics, Incident Response (DFIR), and Threat Hunting, with over 6 years dedicated to actively defending against threats, leading response efforts, and conducting deep forensic investigations. He has worked across diverse industries including healthcare, pharmaceutical, manufacturing, legal, and financial sectors, helping organizations detect, contain, and recover from complex security incidents. By day, he serves as a senior Incident Response case manager and consultant, conducting investigations, leading threat hunts, or mentoring clients on how to build and run effective incident response teams. He brings a hands-on, analytical approach to defending infrastructure and uncovering adversary tradecraft. Outside of work, Kainu is a passionate locksport practitioner and a proud #GirlDad, driven by curiosity, resilience, and a commitment to protecting what matters most.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Threat Hunting Explained Badly

Tags: Blue Team Village | Creator Talk/Panel

When: Saturday, Aug 8, 15:45 - 16:45 PDT

Where: LVCCW Level 2 W217 (Blue Team Village) Main Stage - [Map](#)

Description:

Modern threat hunting is messy. AI lies. Telemetry sucks. Your vibe-coded query returns 12 million rows. Come hear hunters argue about what actually works, what doesn't, and whether any of us agree on what "threat hunting" even means.

Speakers: Alllison Gallo, Brian Baskin, Silas Cutler, Sydney "letswastetime" Marrone

SpeakerBio: Alllison Gallo

Allison Gallo is a staff incident responder on Splunk's Advanced Response Team, where she leads investigations end to end. She entered cybersecurity over a decade ago as a sysadmin at an MSSP, where every day brought a different client and environment, and has since worked as an analyst, consultant, and team lead across agriscience and software.

Incident response is her home, but she's spent time working the other side of the same problem: hunting threats at large-scale events including the Super Bowl, GovWare Singapore, and RSAC. She's convinced the reactive and proactive halves of defense sharpen each other and every incident teaches you what to hunt for next. When not working, she's likely to be on a beach or mountain with her family.

SpeakerBio: Brian Baskin

Brian Baskin is a Threat Researcher for Sublime Security with a specialty in incident response, threat hunting, and malware analysis. Baskin was previously an intrusions analyst for the US Defense Cyber Crime Center (DC3) and a threat research lead at Carbon Black's Threat Analysis Unit (TAU). He has authored multiple security books and develops open source tools for more efficient IR and malware analysis.

SpeakerBio: Silas Cutler

Silas Cutler is a Principal Security Researcher at Censys, where he brings over a decade of experience tracking organized cyber threat groups and developing advanced methods for pursuing them. His research connects technical findings to the broader operations behind them, from attacker motivations to active campaigns, covering threats such as the BeaverTail malware tied to North Korea's covert IT-worker operations, the pro-Russian DDoSia (NoName057(16)) platform, and Secret Blizzard APT activity.

Before Censys, Silas held roles focused on malware analysis, reverse engineering and adversary tracking, including Resident Hacker at Stairwell, Reverse Engineering Lead at Google Chronicle, and Senior Security Researcher on CrowdStrike's Intelligence team. Across these roles, he has specialized in analyzing tools built by nation-state and organized cybercrime groups and developing the methods needed to track them at scale. He is also an active contributor to the wider security research community, sharing his work through conference talks and open-source tooling.

Silas is also the founder and lead developer of MalShare, a public malware repository that has provided the global security research community with free, open access to malware samples since 2013.

SpeakerBio: Sydney "letswastetime" Marrone

Sydney Marrone is a threat hunter, SANS course author, co-founder of THOR Collective, author of the Agentic Threat Hunting Framework (ATHF), and co-author of the PEAK Threat Hunting Framework. She is passionate about helping defenders become better threat hunters by turning complex ideas into practical, repeatable techniques. Through open-source research, workshops, and community-driven projects, Sydney builds frameworks and resources that make hunting more structured, collaborative, and effective. Outside of work, she writes for THOR Collective Dispatch, lifts weights, and makes cyber-inspired music with AI.

--

Sydney Marrone is a threat hunter, cybersecurity professional, co-founder of THOR Collective, author of the Agentic Threat Hunting Framework, and co-author of the PEAK Threat Hunting Framework. She is passionate about making security knowledge accessible and actionable through hands-on research, open-source collaboration, and community-driven projects like HEARTH (Hunting Exchange And Research Threat Hub). Sydney creates resources, leads workshops, and shares insights that spark curiosity and empower defenders. Outside of work, she writes for THOR Collective Dispatch, lifts weights, and makes cyber-themed music using AI to blend creativity and hacker culture.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Threat Hunting in OT Networks - Using Hypothesis Based Methods

Tags: ICS Village | Creator Talk/Panel

When: Friday, Aug 7, 12:00 - 12:30 PDT

Where: LVCCW Level 1 Hall 3 801 (Creator Stage 1) - [Map](#)

Description:

Operational Technology (OT) networks present unique challenges for cybersecurity professionals tasked with detecting and mitigating threats. These networks, often critical to industrial control systems and infrastructure, require specialized approaches due to their complexity, legacy systems, and operational sensitivities. This presentation explores the art and science of threat hunting in OT environments, emphasizing the use of hypothesis-based methods to uncover hidden adversaries and anomalous behaviors.

Attendees will gain insight into the special considerations and hazards associated with OT networks, including safety-critical systems, real-time constraints, and the potential for operational disruption. The talk will also provide a structured approach to hypothesis development, testing, and refinement, enabling practitioners to systematically investigate potential threats with minimal impact on operations.

Finally, the presentation will delve into the practical logistical steps required to conduct threat hunts and incident response (IR) in OT environments, addressing challenges such as network segmentation, communication protocols, and coordination with operational teams. Whether you're a seasoned cybersecurity professional or new to OT security, this discussion will equip you with actionable strategies for effectively hunting threats in these critical and often misunderstood environments.

SpeakerBio: Michael Cardwell, INL

Michael Cardwell is a Cybersecurity Analyst and Researcher for the OT Hunt and Incident Response team at the INL. He has officially worked at the Lab since 2016 and has held various positions at the lab. One of the highlights of his time at the lab includes being the technical lead for the development of the Malcolm tool, which is a threat hunting tool suite developed at the INL for OT threat hunting. He has participated in hunts, IR's and assessments in OT networks.

Prior to working at the Lab he was an ISSO (Information System Security Officer). He also worked in the private sector as an IT Security Administrator for 10 years before that.

He holds degrees in Electronics, Computer Science, and Cybersecurity. He currently lives in Idaho with his wife, 2 children and lots of cats.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Blue Team Village - Saturday - 13:15-14:15 PDT

Title: Threat Intelligence in Real Life

Tags: Blue Team Village | Creator Talk/Panel

When: Saturday, Aug 8, 13:15 - 14:15 PDT

Where: LVCCW Level 2 W217 (Blue Team Village) Main Stage - [Map](#)

Description:

Correlation, causation, and the occasional compromise that cost us a weekend. This panel trades the talk slides for an open discussion of the realities of threat intelligence practice: the dead ends, the misread infrastructure, the cluster that fell apart under scrutiny, and the overlapping TTPs that finally tied things together. Our panel of practitioners engages the audience with real cases, separating nation-state from cybercrime by intent and tradecraft, tracking infrastructure, and catching the logical fallacies that quietly steer analysis wrong. We'll talk about how the work really gets done, where confident analysis quietly goes sideways, and the industry challenges on the horizon.

Speakers: Ashley Sequeira, Julian Zottl, Leigh Gilbert, Madeline Sedgwick

SpeakerBio: Ashley Sequeira

Ashley is a cybersecurity researcher, threat intelligence practitioner, and Senior Sales Engineer at Censys, where she conducts strategic research on IoT botnets and adversarial infrastructure. Her research sits at the intersection of hardware-based attack infrastructure and influence operations, tracking how low-cost consumer electronics are weaponized as residential proxy networks, ad fraud engines, and persistent footholds inside homes and enterprise networks.

SpeakerBio: Julian Zottl

Julian Zottl is the Chief Technology Officer for AzgardTek, an engineering company focused on Cyber and Intelligence. He's the former CTO of Cyber Protection Solutions within Raytheon Intelligence & Space, a Raytheon Technologies business. He is also Cyber and Information Operations (IO) Subject Matter Expert (SME) and considered a world expert in large scale Computer Network Defense (CND).

SpeakerBio: Leigh Gilbert, Malware village

Leigh Trinity is a Canadian exploit developer, red team hacker, and instructor known for her work in binary exploitation and reverse engineering. Now branching out into malware development.

SpeakerBio: Madeline Sedgwick

Madeline Sedgwick is a Principal Threat Researcher at Palo Alto Networks Unit 42's National Security Team, focusing on South Asian threat actors and covert networks. In her 13 years of professional experience, Madeline has worked on all sides of the cyber front: military, government, and private sector. Her mission, inspired by years of ruined holiday weekends at the Department of Defense, is to make the other guys work the weekend.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

The Diana Initiative - Sunday - 11:00-12:59 PDT

Title: Threat Model your Career Workshop

Tags: The Diana Initiative | Creator Event/Activity

When: Sunday, Aug 9, 11:00 - 12:59 PDT

Where: LVCCW Level 2 W209 (Diana Initiative) - [Map](#)

Description:

We threat model systems all the time. Almost nobody runs that same thinking on their own career, which is usually the most valuable thing they own. Let's spend two hours looking at your career the way you would look at something you are paid to defend: what is worth protecting, what could go wrong, where they are exposed, and what you are actually going to do about it.

Everyone will leave with a filled-in canvas and one specific thing they have committed to in the next month. This workshop is for any experience level.

SpeakerBio: Chandan Vedavyas

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Threat Modeling LLMs with PHANTOM-B

Tags: Intermediate | AppSec Village | Creator Talk/Panel

When: Saturday, Aug 8, 12:30 - 12:59 PDT

Where: LVCCW Level 1 Hall 2 604 (Appsec Village) Main Stage - [Map](#)

Description:

Threat modeling systems that call LLMs requires specialized approaches. Existing frameworks are heavyweight (wordy, jargon-laden) and often focus on threats that can only be addressed by those who train the models, offering little help to security practitioners tasked with threat modeling their company's latest AI feature or product. This talk will introduce PHANTOM-B a new, STRIDE-like mnemonic for threat modeling LLMs. PHANTOM-B is focused on the common case of "an LLM trained by others," rather than those training the LLM themselves.

SpeakerBio: Adam Shostack

Adam is leading expert on threat modeling and secure by design. He currently helps many organizations improve their security by with training and coaching at Shostack + Associates. He's the author of Threats: What Every Engineer Should Learn from Star Wars, Threat Modeling: Designing for Security and The New School of Information Security (with Andrew Stewart). He's a member of the BlackHat Review Board, and helped create the CVE and many other things, and is an Affiliate Professor at the University of Washington.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Threatmaxxing Your Stakeholders while Mogging Your Threat Actors: What is Cyber Threat Intel?

Tags: Noob Community | Creator Talk/Panel

When: Friday, Aug 7, 13:00 - 13:15 PDT

Where: LVCCW Level 1 Hall 4 1417 (Noob Community) - [Map](#)

Description:

This is a 15 minute lightning talk with an intro/brief overview of the Cyber Threat Intelligence discipline. Topics covered include why it's so hard to identify and define what CTI is in the current industry, the different aspects of what can be expected from CTI, and the typical backgrounds of CTI practitioners.

Having been a part of CTI teams at organizations with a wide variety of resources and maturity levels, this talk provides a realistic, ground-level view of the industry and what your average CTI experience is like, not the curated experiences of Fortune 500 CTI teams we all see presenting on the main stage.

SpeakerBio: Eli Woodward, Senior Threat Intelligence Advisor with Team Cymru

Eli Woodward is a cyber threat intelligence advisor with Team Cymru. He's worked in a variety of industries including financial services and government, and has seen the range of organizations from extremely well-resourced and capable to the shoestring budget. This has given him unique insights into CTI at all levels of complexity, maturity, and resources. He holds a master's degree in Intelligence and Security Studies and also plays bagpipes competitively.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: ThreatPatrol: Visualising the Modern Threat Landscape

Tags: ICS Village | Creator Talk/Panel

When: Sunday, Aug 9, 12:00 - 12:30 PDT

Where: LVCCW Level 1 Hall 3 801 (Creator Stage 1) - [Map](#)

Description:

ThreatPatrol is a modern, open-source SaaS platform designed to operationalise cyber threat intelligence across Blue Teams, Cyber Threat Intelligence (CTI) analysts, Atomic Engineers and Purple Teams. Built natively around the MITRE ATT&CK framework and enriched with ART Atomic Red Team mappings, ThreatPatrol bridges the long-standing gap between threat intelligence, detection engineering and adversary simulation.

Unlike traditional CTI platforms that focus solely on indicators or static reporting, ThreatPatrol consolidates campaigns, adversary behaviour, atomic tests, infrastructure and detection analytics into a unified, relational data model. This enables practitioners to move beyond passive intelligence consumption toward active defense validation, threat emulation and measurable security outcomes.

The platform provides deep correlation across:

- Threat actors, campaigns and malware
- ATT&CK tactics, techniques, and procedures (TTPs)
- Atomic tests and adversary emulation workflows
- Detection logic and security controls
- Infrastructure and industry-specific threat exposure canvas
- ICS & IOT systems mapping with various framework on a 3D canvas

ThreatPatrol allows teams to:

- Map real-world adversary campaigns across the ATT&CK kill chain
- Emulate attacker behaviour using validated atomic tests
- Identify detection blind spots via contextual GAP analysis
- Visualise relationships between threats, tooling and mitigations
- Improve detection engineering aligned to adversary tradecraft
- Mature threat hunting with intelligence-led prioritisation
- Analyse threats targeting modern technologies such as AI agents and MCP ecosystems
- Extend visibility into ICS and IOT devices and industry-specific attack surfaces
- Mapping of each components of ICS and IOT devices to NIST, MITRE, Australian Standards, DoD Essential eight framework

The platform ships with:

- 160+ curated threat actor profiles
- 100+ live threat intelligence feeds
- 20+ ICS and SOCI industry related Threat Canvas on 3D HoloLens
- 20+ IOT Devices Component level attacks
- Continuously updated campaign and TTP mappings
- ATT&CK-aligned detection and mitigation coverage
- Campaign visualisation and attack path analysis tools
- Support for custom atomic tests and adversary simulation scripts

ThreatPatrol is designed for continuous adversary-driven security validation, enabling organisations to test, measure, and improve their resilience against realistic attack scenarios. By transforming fragmented intelligence into actionable, visual and testable insights, ThreatPatrol provides a single platform for understanding, simulating and defending against modern cyber threats.

SpeakerBio: Viral Maniar, UniSuper

Viral Maniar is a Senior Security Specialist at UniSuper, responsible for leading the organisation's offensive and defensive security services within the information security team. He also operates his boutique cybersecurity firm, Preemptive Cybersecurity based in Australia, delivering both offensive and defensive security consulting services. With over thirteen years of experience in cybersecurity consulting, Viral has worked with a wide range of organisations across APJ. His expertise includes internal and external infrastructure testing, application penetration testing, vulnerability assessments, wireless security assessments, social engineering, red teaming, API testing, thick and thin client testing, and cloud security architecture reviews. Viral has spoken at prominent industry conferences such as Black Hat, ROOTCON DEFCON and (ISC)². He is also an active participant in bug bounty programs and has received recognition for responsibly disclosing security vulnerabilities. Outside of his professional work, Viral enjoys building security tools and contributes to multiple projects on GitHub. He can be found on X at @ManiarViral and @PreemptiveCyber.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Threats in Space: The Dangerous Rise of GNSS Attacks

Tags: Telecom Village | Creator Talk/Panel

When: Saturday, Aug 8, 11:00 - 11:45 PDT

Where: LVCCW Level 3 W321 (Telecom Village) - [Map](#)

Description:

1. GNSS constellations
2. How do we use GNSS daily?
3. GNSS threats and their rise
4. Hactivism and GNSS?
5. GNSS exposed instances over the internet
6. Can we defend against GNSS attacks

SpeakerBio: Isabel Manjarrez, Threat Researcher

[EN] María Isabel Manjarrez is a security researcher with Kaspersky's Global Research and Analysis Team (GReAT). She specializes in investigating threat actors in Latin America, tracking their movements, and analyzing the new techniques they deploy. She holds a degree in telecommunications and electronic systems engineering and her interests include threat intelligence, malware analysis, satellite communications, electronics, and music.

She has shared her knowledge as a speaker at local and international conferences such as Defcon, Security Analyst Summit (SAS), and EkoParty.

[ES] María Isabel Manjarrez es investigadora de seguridad en el Equipo Global de Investigación y Análisis (GReAT) de Kaspersky. Se especializa en la investigación de actores amenaza en Latinoamérica, rastrea sus movimientos y analiza las nuevas técnicas que implementan. Es Ingeniera en telecomunicaciones y sistemas electrónicos, sus intereses incluyen la inteligencia de amenazas, análisis de malware, comunicaciones satelitales, electrónica y música.

Ha compartido su conocimiento como ponente en conferencias locales e internacionales como Defcon, Security Analyst Summit (SAS) y EkoParty.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Throw Out the Alphabet: Token-Based Markov Chains for Password Cracking

Tags: DEF CON Official Talk | Tool

When: Saturday, Aug 8, 15:00 - 15:59 PDT

Where: LVCCW Level 1 Hall 3 1006 (Main Track 1) - [Map](#)

Description:

Classical Markov password generators work over the character alphabet: hashcat's Markov masks, JtR's --markov, OMEN, even neural models like PassGPT.

We change one thing: the alphabet. Train an n-gram Markov on RockYou, but segment with GPT-2's 50k BPE tokenizer instead of characters. The distribution stays RockYou-derived; only the units change. The vocabulary captures structure characters can't: name fragments, digit patterns, symbol clusters from web-scale text.

Across 14 leak corpora (RockYou, LinkedIn, Yahoo, +11 more), token-Markov beats OMEN at fixed budgets on all 14, at 10^8 and 10^9 , with best66 rules on both sides. On enterprise passwords (8+ chars, 3 of 4 classes), we recover ~6x more than OMEN: 6.3% vs 1.1% at 10^8 , 12.3% vs 2.3% at 10^9 ; the lead holds ~2.8x with rules applied. tokenov hits 10^9 candidates in minutes on CPU; OMEN takes hours; PassGPT needs days.

Why: the tokenizer bakes in mixed-case, digit, and symbol primitives, so multi-class compliance is modal, not rare. "Michael99" is two tokens, not eight transitions.

We release tokenov: train an n-gram model with any tokenizer, or use include custom GTP-2 tokenizer. Pipe into hashcat, JtR, or write to disk. Use OSINT derived lists to seed generation customized to the target. No GPU needed: 1B candidates in under 2 minutes on an i9.

- Narayanan & Shmatikov, "Fast dictionary attacks on passwords using time-space tradeoff," CCS 2005. (Markov password modeling, original.)
- Weir et al., "Password cracking using probabilistic context-free grammars," IEEE S&P 2009. (PCFG, the natural rival to Markov.)
- Durmuth et al., "OMEN: Faster password guessing using an ordered Markov enumerator," ESSoS 2015. (The level-ordered enumerator we benchmark against.)
- Melicher et al., "Fast, lean, and accurate: Modeling password guessability using neural networks," USENIX Security 2016. (FLA, the neural baseline.)
- Hitaj et al., "PassGAN: A deep learning approach for password guessing," ACNS 2019.
- Rando et al., "PassGPT: Password modeling and (guided) generation with LLMs," ESORICS 2023. (Closest prior work; uses GPT-2 fine-tuned on RockYou. We outperform it.)
- Cracken (<https://github.com/shmuelamar/cracken>). The proximate inspiration; uses BPE for password masks. We extend the BPE idea from masks to full Markov generation.
- MAYA benchmark (S&P 2026). The 19-corpus evaluation framework we adopted.

SpeakerBio: Jon "flakpaket" Gorenflo, ATTACKD

Jon Gorenflo is the founder of ATTACKD, a cybersecurity consulting firm dedicated to helping organizations of all sizes think like attackers and proactively secure their environments. Whether you're a startup, a small business, or a global enterprise, Jon brings real-world offensive security insights that are practical, accessible, and actionable. He is also a Principal Instructor with the SANS Institute and the co-author of SEC560: Enterprise Penetration Testing, a leading course on advanced ethical hacking and red team operations. With more than 20 years of combined experience in IT, penetration testing, incident response, and security training, Jon has worked with a diverse range of organizations to uncover critical vulnerabilities and build resilient defenses. In addition, Jon serves as the executive director of Hackers Teaching Hackers (HTH), a grassroots cybersecurity conference that emphasizes hands-on learning and community connection. Jon is known for his clear communication, relatable style, and dedication to helping defenders build practical skills. He breaks down hacker tactics into

understandable steps and helps teams of all sizes, from a solo IT admin to an enterprise SOC, apply those lessons to real-world defenses.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Contests - Sunday - 10:00-11:59 PDT

Title: Tin Foil Hat Contest

Tags: Tin Foil Hat Contest | Contest

When: Sunday, Aug 9, 10:00 - 11:59 PDT

Where: LVCCW Level 1 Hall 1 403 (Tin Foil Hat Contest) - [Map](#)

Description:

Want to protect your noggin from government mind control rays? Have you angered our new AI Overlords, and now need to hide? Maybe those alien brainwave blasters just have you feeling down lately? Or do you just want to do something fun and forget about the world's woes for a while? Fear not, for we here at the Tin Foil Hat Contest have your back for all of these! Come find us in the contest area, and we'll have you build a tin foil hat which is guaranteed to provide top quality protection for your cerebellum . How you ask? SCIENCE!

Show us your skills by building a tin foil hat to shield your subversive thoughts, then test it out for effectiveness.

There are 2 categories: stock and unlimited. The hat in each category that causes the most signal attenuation will receive the ""Substance"" award for that category. We all know that hacker culture is all about looking good though, so a single winner will be selected for ""Style"". We provide all contestants a meter of foil, but you're welcome to acquire and use as much as you want from other sources.

This year is dedicated to our brother & contest creator, Flirzan. We'll never forget drunkenly hashing this out on a napkin with you at DEFCON many years ago. Rest in peace, we miss you friend!

Participant Prerequisites

We supply the base materials to participate. Contestants are welcome to bring additional foil if they desire.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Contests - Saturday - 10:00-17:59 PDT

Title: Tin Foil Hat Contest

Tags: Tin Foil Hat Contest | Contest

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 403 (Tin Foil Hat Contest) - [Map](#)

Description:

Want to protect your noggin from government mind control rays? Have you angered our new AI Overlords, and now need to hide? Maybe those alien brainwave blasters just have you feeling down lately? Or do you just want to do something fun and forget about the world's woes for a while? Fear not, for we here at the Tin Foil Hat Contest have your back for all of these! Come find us in the contest area, and we'll have you build a tin foil hat which is guaranteed to provide top quality protection for your cerebellum . How you ask? SCIENCE!

Show us your skills by building a tin foil hat to shield your subversive thoughts, then test it out for effectiveness.

There are 2 categories: stock and unlimited. The hat in each category that causes the most signal attenuation will receive the ""Substance"" award for that category. We all know that hacker culture is all about looking good though, so a single winner will be selected for ""Style"". We provide all contestants a meter of foil, but you're welcome to acquire and use as much as you want from other sources.

This year is dedicated to our brother & contest creator, Flirzan. We'll never forget drunkenly hashing this out on a napkin with you at DEFCON many years ago. Rest in peace, we miss you friend!

Participant Prerequisites

We supply the base materials to participate. Contestants are welcome to bring additional foil if they desire.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Contests - Friday - 10:00-17:59 PDT

Title: Tin Foil Hat Contest

Tags: Tin Foil Hat Contest | Contest

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 403 (Tin Foil Hat Contest) - [Map](#)

Description:

Want to protect your noggin from government mind control rays? Have you angered our new AI Overlords, and now need to hide? Maybe those alien brainwave blasters just have you feeling down lately? Or do you just want to do something fun and forget about the world's woes for a while? Fear not, for we here at the Tin Foil Hat Contest have your back for all of these! Come find us in the contest area, and we'll have you build a tin foil hat which is guaranteed to provide top quality protection for your cerebellum . How you ask? SCIENCE!

Show us your skills by building a tin foil hat to shield your subversive thoughts, then test it out for effectiveness.

There are 2 categories: stock and unlimited. The hat in each category that causes the most signal attenuation will receive the ""Substance"" award for that category. We all know that hacker culture is all about looking good though, so a single winner will be selected for ""Style"". We provide all contestants a meter of foil, but you're welcome to acquire and use as much as you want from other sources.

This year is dedicated to our brother & contest creator, Flirzan. We'll never forget drunkenly hashing this out on a napkin with you at DEFCON many years ago. Rest in peace, we miss you friend!

Participant Prerequisites

We supply the base materials to participate. Contestants are welcome to bring additional foil if they desire.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: To Catch a Pseudoscientist

Tags: Biohacking Village | Creator Talk/Panel

When: Saturday, Aug 8, 10:00 - 10:30 PDT

Where: LVCCW Level 1 Hall 3 1104 (Creator Stage 4) - [Map](#)

Description:

This talk exposes the hidden fraud ecosystem inside modern scientific research, where paywalls, paper mills, predatory journals, and fake credentials create the illusion of legitimacy. Drawing from a hacker's perspective, it examines how corruption is embedded in the system, how some actors knowingly participate while others are trapped by it, and how weak or fabricated work can be elevated as credible science. The session offers a practical playbook for identifying red flags, avoiding fraudulent channels, and protecting yourself from the pipeline where fake journals produce fake science.

SpeakerBio: James Utley PhD

Dr. James Utley, PhD is a board-certified anti-aging scientist and immunohematology expert advancing AI, regenerative medicine, and cellular reprogramming. As CSO at Auragens, he develops stem cell therapeutics, translating molecular science into clinical strategies to extend healthspan.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: TokenMesh: Exposing Azure's Hidden Identity Attack Surface

Tags: AI | DEF CON Demo Labs | Intermediate | Cloud | Defense/Blue Team | Offense/Red Team | DEF CON Demo Labs

When: Friday, Aug 7, 15:00 - 15:45 PDT

Where: LVCCW Level 1 Hall 3 901 (Demo Labs Track 5) - [Map](#)

Description:

Modern cloud environments are riddled with identity misconfigurations that go undetected until it's too late. TokenMesh is an open-source Azure security reconnaissance tool built to expose exactly that — over-privileged identities, dormant service principals, misconfigured storage accounts, and potential backdoors hiding in plain sight across Microsoft Entra ID and Azure RBAC. Unlike traditional scanners that drown you in raw data, TokenMesh is designed with the security practitioner in mind. It integrates directly with the Model Context Protocol (MCP) and the OpenAI API, allowing AI-assisted analysis that surfaces critical findings in plain language — no SIEM required, no query language to master. Plug it into your AI workflow of choice, ask questions in natural language, and get answers that actually make sense. In this session, we'll walk through how TokenMesh was built, the real-world attack paths it uncovers, and live demonstrations against a target Azure environment. We'll cover how attackers abuse identity misconfigurations, how privilege escalation paths hide inside legitimate role assignments, and how defenders can use TokenMesh to harden their posture before adversaries exploit it. Whether you're a red teamer mapping an Azure tenant or a blue teamer trying to get ahead of the next breach.

SpeakerBio: Saksham Agrawal

Saksham Agrawal is a Senior Security Consultant at NotSoSecure, specializing in cloud security. His work focuses on discovering new attack paths in cloud environments and helping organizations understand real-world risks. He has presented his research at DEF CON Cloud Village, where he introduced his tool NoPrompt and shared practical techniques for cloud security testing. He enjoys building tools, exploring cloud internals, and sharing his findings with the security community. He has also responsibly reported critical vulnerabilities in major cloud vendors as part of his independent security research and actively delivers training sessions on cloud security and offensive security techniques.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: TokenMesh: Exposing Azure's Hidden Identity Attack Surface

Tags: AI | DEF CON Demo Labs | Intermediate | Cloud | Defense/Blue Team | Offense/Red Team | DEF CON Demo Labs

When: Saturday, Aug 8, 11:00 - 11:45 PDT

Where: LVCCW Level 1 Hall 3 901 (Demo Labs Track 5) - [Map](#)

Description:

Modern cloud environments are riddled with identity misconfigurations that go undetected until it's too late. TokenMesh is an open-source Azure security reconnaissance tool built to expose exactly that — over-privileged identities, dormant service principals, misconfigured storage accounts, and potential backdoors hiding in plain sight across Microsoft Entra ID and Azure RBAC. Unlike traditional scanners that drown you in raw data, TokenMesh is designed with the security practitioner in mind. It integrates directly with the Model Context Protocol (MCP) and the OpenAI API, allowing AI-assisted analysis that surfaces critical findings in plain language — no SIEM required, no query language to master. Plug it into your AI workflow of choice, ask questions in natural language, and get answers that actually make sense. In this session, we'll walk through how TokenMesh was built, the real-world attack paths it uncovers, and live demonstrations against a target Azure environment. We'll cover how attackers abuse identity misconfigurations, how privilege escalation paths hide inside legitimate role assignments, and how defenders can use TokenMesh to harden their posture before adversaries exploit it. Whether you're a red teamer mapping an Azure tenant or a blue teamer trying to get ahead of the next breach.

SpeakerBio: Saksham Agrawal

Saksham Agrawal is a Senior Security Consultant at NotSoSecure, specializing in cloud security. His work focuses on discovering new attack paths in cloud environments and helping organizations understand real-world risks. He has presented his research at DEF CON Cloud Village, where he introduced his tool NoPrompt and shared practical techniques for cloud security testing. He enjoys building tools, exploring cloud internals, and sharing his findings with the security community. He has also responsibly reported critical vulnerabilities in major cloud vendors as part of his independent security research and actively delivers training sessions on cloud security and offensive security techniques.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Tokens and PRT: Advanced Attacks and Persistence in Microsoft Entra ID

Tags: Cloud Village | Creator Talk/Panel

When: Friday, Aug 7, 10:50 - 11:30 PDT

Where: LVCCW Level 3 W313 (Cloud Village Talks) - [Map](#)

Description:

Is MFA and Conditional Access a real security guarantee? In this technical session, we will demonstrate how endpoint compromise allows an attacker to bypass traditional identity barriers in the cloud. The talk focuses on exploiting vulnerabilities in Microsoft Entra ID, breaking down an advanced attack chain:

- Device Code Flow: Abuse of authentication flows for initial access (Demo with Entraith).
- PowerShell Hijacking: Process interception to obtain session tokens (GrabTokenAzureAD).
- Sliver BOF Extraction: Use of Beacon Object Files (BOF) for stealthy exfiltration of tokens and the Primary Refresh Token (PRT) from memory, evading anti-malware defenses.
- MFA Bypass and Intune: Custom tools were developed to extract local PRTs, bypass Intune device management controls, and circumvent MFA. The entire process was automated through the open-source tool <https://github.com/bl4ckskull1/entraith>, enabling attacks via device code flow, token renewal, email and app inspection, token exfiltration, and persistence generation.

Speakers: Elzer Pineda, Jose Rivas

SpeakerBio: Elzer Pineda, Pentester

Regional Pentester and Cybersecurity Consultant, Elzer Pineda is an active member of the Red Team executing strategic consulting projects and advanced penetration testing engagements. His career has been focused on Threat Research for private and government organizations across the region. He is a Dojo Community Ambassador and Professor at the Universidad Tecnológica de Panamá (UTP). His experience has taken him to share technical research at Ekoparty, BSides Latam Peru, BSides Panamá, DOJOConf, PwnedCR, and OWASP Latam. Offensive security certifications: OSWE, OSEP, OSCP, OSWP, CRTP, CRT0, and CRTL.

--

Profesor en la Universidad Tecnológica de Panamá y especialista en Red Team con más de 10 años de experiencia en ciberseguridad ofensiva y defensiva. Pentester en GBM (región y Estados Unidos) y researcher en Toad Security. Máster en Seguridad Informática. Realiza evaluaciones de seguridad a aplicaciones móviles, web e infraestructura en Latinoamérica y comparte activamente conocimientos en la comunidad Dojo como embajador y conferencias. Certificaciones: OSWE, OSEP, OSCP, CRT0, OSWP, CRTL.

SpeakerBio: Jose Rivas, Experienced Penetration Tester at A-LIGN

Jose Rivas is an Offensive Security Researcher and Red Team Operator at A-LIGN, specializing in adversarial simulations, Active Directory attack paths, and physical security assessments. Co-founder of Zero Trust Offsec, an offensive security research group focused on vulnerability exploitation, emerging attack techniques, and responsible disclosure, and Founder of DCG Panama, Panama's first official DEF CON chapter, where he leads a community dedicated to red team operations, and adversarial tradecraft. A recognized voice in the Panamanian security community, Jose has spoken at BSides Colombia, BSides Panama, OWASP Panama, and DOJOConf. With certifications including CRT0, eWPT, eCPPT, and CompTIA PenTest+, he brings a threat-actor mindset and a strong commitment to advancing offensive security knowledge across the region.

Jose Manuel Rivas is a Penetration Tester and Red Team Operator at A-LIGN, with hands-on experience in adversarial simulations, Active Directory attack chains, web application testing, and physical security assessments. He has multiple CVEs

to his name, discovered through bug bounty programs and independent vulnerability research. Co-founder of Zero Trust Offsec and founder of DCG Panama, Panama's first official DEF CON chapter. He has spoken at BSides Colombia, BSides Panama, OWASP Panama, and DOJOConf, and is focused on growing the penetration testing and red team culture across Latin America.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Tokens and PRT: Advanced Attacks and Persistence in Microsoft Entra ID

Tags: Red Team Village | Misc

When: Sunday, Aug 9, 10:00 - 11:59 PDT

Where: LVCCW Level 1 Hall 1 309 (Red Team Village) Tactic Table 1 - [Map](#)

Description:

Is MFA and Conditional Access a real security guarantee? In this technical session, we will demonstrate how endpoint compromise allows an attacker to bypass traditional identity barriers in the cloud. The talk focuses on exploiting vulnerabilities in Microsoft Entra ID, breaking down an advanced attack chain:

- Device Code Flow: Abuse of authentication flows for initial access (Demo with Entraith).
- PowerShell Hijacking: Process interception to obtain session tokens (GrabTokenAzureAD).
- Sliver BOF Extraction: Use of Beacon Object Files (BOF) for stealthy exfiltration of tokens and the Primary Refresh Token (PRT) from memory, evading anti-malware defenses.
- MFA Bypass and Intune: The speakers developed custom tooling to extract local PRTs, bypass Intune device management controls, and circumvent MFA. This entire attack lifecycle was consolidated into Entraith — an offensive framework built from scratch by the research team and set to be released publicly at DEF CON 34 (<https://github.com/bl4ckskull1/entraith>) — enabling device code attacks, token renewal, email and app inspection, token exfiltration, and persistence generation from a single interface.

This talk is not about a single CVE or a niche edge case. It is a comprehensive offensive research presentation covering the full spectrum of attack techniques against Microsoft Entra ID — from the very first foothold to deeply rooted, multi-vector persistence that survives incident response.

We will demonstrate, live, how an attacker moves through every phase of an Entra ID compromise:

INITIAL ACCESS AND TOKEN THEFT: We begin with Device Code Flow phishing — abusing Microsoft’s own authentication protocol to harvest valid tokens without ever touching a password. We then escalate with PowerShell process hijacking (GrabTokenAzureAD) to intercept live session tokens, and culminate with Sliver BOF-based extraction of the Primary Refresh Token (PRT) directly from memory — stealthy, silent, and anti-malware evasive. These three techniques alone demonstrate that MFA and Conditional Access are not the guarantees organizations believe them to be.

BYPASSING INTUNE AND MFA: Purpose-built tools developed during this research extract local PRTs, bypass Intune device compliance controls, and circumvent MFA enforcement at the token layer — not through social engineering, but through direct abuse of Microsoft’s identity platform mechanics. Attackers operating from non-enrolled or non-compliant devices can achieve full Tenant access that Conditional Access policies are designed to prevent.

PERSISTENCE ACROSS 10 VECTORS: Once inside, we deploy a “Survival Kit” of 10 chained persistence mechanisms — camouflaged App Registrations, long-lived secrets and certificates, backdoor accounts, strategic role assignments, privileged group inheritance, admin mailbox delegation, inbox-rule-based exfiltration of credentials and MFA codes, OAuth consent grants to external applications, and Temporary Access Pass generation for on-demand MFA bypass. No single blue team action — password reset, MFA enforcement, device wipe — removes all of them simultaneously.

ENTRAITH — BUILT BY US, RELEASED AT DEF CON: The centerpiece of this talk is Entraith (<https://github.com/bl4ckskull1/entraith>), an offensive framework designed and built from the ground up by the speakers specifically for this research. Entraith is not a wrapper around existing tools — it is original work, developed over months of hands-on red team engagements against real Microsoft 365 environments. It unifies every technique demonstrated in this talk into a single operator interface: device code phishing, PRT extraction from memory, Intune compliance bypass, token renewal and exfiltration, email and application enumeration, and the full 10-step persistence deployment chain. DEF CON 34 will be the moment Entraith is released to the public. Attendees will be among the first to access the tool, its documentation, and the full methodology behind it — making this talk a genuine first-look at original research with immediate real-world impact.

WHY THIS MATTERS FOR CLOUD VILLAGE: The Microsoft 365 and Entra ID ecosystem is the identity backbone of the majority of enterprise organizations worldwide. The techniques presented here are not theoretical — they are being used by real threat actors today. Defenders in the room will leave with concrete detection opportunities and an understanding of exactly which log sources and control gaps allow this attack chain to succeed undetected. Red teamers will leave with a working tool and a fully documented methodology. This talk delivers both offensive depth and defensive utility in a single session, and the live demos ensure no attendee has to take our word for it.

Speakers: Elzer Pineda, Jose Rivas

SpeakerBio: Elzer Pineda, Pentester

Regional Pentester and Cybersecurity Consultant, Elzer Pineda is an active member of the Red Team executing strategic consulting projects and advanced penetration testing engagements. His career has been focused on Threat Research for private and government organizations across the region. He is a Dojo Community Ambassador and Professor at the Universidad Tecnológica de Panamá (UTP). His experience has taken him to share technical research at Ekoparty, BSides Latam Peru, BSides Panamá, DOJOConf, PwnedCR, and OWASP Latam. Offensive security certifications: OSWE, OSEP, OSCP, OSWP, CRTP, CRTO, and CRTL.

--

Profesor en la Universidad Tecnológica de Panamá y especialista en Red Team con más de 10 años de experiencia en ciberseguridad ofensiva y defensiva. Pentester en GBM (región y Estados Unidos) y researcher en Toad Security. Máster en Seguridad Informática. Realiza evaluaciones de seguridad a aplicaciones móviles, web e infraestructura en Latinoamérica y comparte activamente conocimientos en la comunidad Dojo como embajador y conferencias. Certificaciones: OSWE, OSEP, OSCP, CRTO, OSWP, CRTL.

SpeakerBio: Jose Rivas, Experienced Penetration Tester at A-LIGN

Jose Rivas is an Offensive Security Researcher and Red Team Operator at A-LIGN, specializing in adversarial simulations, Active Directory attack paths, and physical security assessments. Co-founder of Zero Trust Offsec, an offensive security research group focused on vulnerability exploitation, emerging attack techniques, and responsible disclosure, and Founder of DCG Panama, Panama's first official DEF CON chapter, where he leads a community dedicated to red team operations, and adversarial tradecraft. A recognized voice in the Panamanian security community, Jose has spoken at BSides Colombia, BSides Panama, OWASP Panama, and DOJOConf. With certifications including CRTO, eWPT, eCPPT, and CompTIA PenTest+, he brings a threat-actor mindset and a strong commitment to advancing offensive security knowledge across the region.

Jose Manuel Rivas is a Penetration Tester and Red Team Operator at A-LIGN, with hands-on experience in adversarial simulations, Active Directory attack chains, web application testing, and physical security assessments. He has multiple CVEs to his name, discovered through bug bounty programs and independent vulnerability research. Co-founder of Zero Trust Offsec and founder of DCG Panama, Panama's first official DEF CON chapter. He has spoken at BSides Colombia, BSides Panama, OWASP Panama, and DOJOConf, and is focused on growing the penetration testing and red team culture across Latin America.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Tokens and PRT: Advanced Attacks and Persistence in Microsoft Entra ID

Tags: La Villa Community | Creator Talk/Panel

When: Friday, Aug 7, 17:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 4 1416 (La Villa Community) Main Stage - [Map](#)

Description:

¿Son el MFA y el Acceso Condicional una garantía de seguridad real? En esta sesión técnica, demostraremos cómo el compromiso de un endpoint permite a un atacante saltarse las barreras de identidad tradicionales en la nube. La charla se centra en la explotación de vulnerabilidades en Microsoft Entra ID, desglosando una cadena de ataque avanzada:

Abuso de Device Code Flow: Explotación de flujos de autenticación para acceso inicial (Demo con Entraith).

PowerShell Hijacking: Intercepción de procesos para la obtención de tokens de sesión (GrabTokenAzureAD).

Extracción con Sliver BOF: Uso de Beacon Object Files para la exfiltración sigilosa de tokens y del Primary Refresh Token (PRT) directamente desde la memoria, evadiendo defensas anti-malware.

Bypass de MFA e Intune: Hemos desarrollado herramientas personalizadas para extraer PRTs locales, eludir los controles de gestión de dispositivos de Intune y saltarse la aplicación de MFA a nivel de token.

Todo este ciclo de vida de ataque ha sido consolidado en Entraith, un framework ofensivo desarrollado desde cero por nuestro equipo de investigación que será lanzado públicamente en DEF CON 34. Entraith permite ejecutar ataques de device code, renovación de tokens, inspección de correos/aplicaciones y generación de persistencia multi-vector desde una única interfaz

Speakers: Elzer Pineda, Jose Rivas

SpeakerBio: Elzer Pineda, Pentester

Regional Pentester and Cybersecurity Consultant, Elzer Pineda is an active member of the Red Team executing strategic consulting projects and advanced penetration testing engagements. His career has been focused on Threat Research for private and government organizations across the region. He is a Dojo Community Ambassador and Professor at the Universidad Tecnológica de Panamá (UTP). His experience has taken him to share technical research at Ekoparty, BSides Latam Peru, BSides Panamá, DOJOConf, PwnedCR, and OWASP Latam. Offensive security certifications: OSWE, OSEP, OSCP, OSWP, CRTP, CRTO, and CRTL.

--

Profesor en la Universidad Tecnológica de Panamá y especialista en Red Team con más de 10 años de experiencia en ciberseguridad ofensiva y defensiva. Pentester en GBM (región y Estados Unidos) y researcher en Toad Security. Máster en Seguridad Informática. Realiza evaluaciones de seguridad a aplicaciones móviles, web e infraestructura en Latinoamérica y comparte activamente conocimientos en la comunidad Dojo como embajador y conferencias. Certificaciones: OSWE, OSEP, OSCP, CRTO, OSWP, CRTL.

SpeakerBio: Jose Rivas, Experienced Penetration Tester at A-LIGN

Jose Rivas is an Offensive Security Researcher and Red Team Operator at A-LIGN, specializing in adversarial simulations, Active Directory attack paths, and physical security assessments. Co-founder of Zero Trust Offsec, an offensive security research group focused on vulnerability exploitation, emerging attack techniques, and responsible disclosure, and Founder of DCG Panama, Panama's first official DEF CON chapter, where he leads a community dedicated to red team operations, and

adversarial tradecraft. A recognized voice in the Panamanian security community, Jose has spoken at BSides Colombia, BSides Panama, OWASP Panama, and DOJOConf. With certifications including CRT0, eWPT, eCPPT, and CompTIA PenTest+, he brings a threat-actor mindset and a strong commitment to advancing offensive security knowledge across the region.

Jose Manuel Rivas is a Penetration Tester and Red Team Operator at A-LIGN, with hands-on experience in adversarial simulations, Active Directory attack chains, web application testing, and physical security assessments. He has multiple CVEs to his name, discovered through bug bounty programs and independent vulnerability research. Co-founder of Zero Trust Offsec and founder of DCG Panama, Panama's first official DEF CON chapter. He has spoken at BSides Colombia, BSides Panama, OWASP Panama, and DOJOConf, and is focused on growing the penetration testing and red team culture across Latin America.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Hackers.town - Friday - 14:00-14:59 PDT

Title: Too Much "Slop" and Not Enough Soul: Why the AI Music Bubble is Leaking & Robots Shouldn't Replace Our Djs

Tags: Hackers.town | Creator Talk/Panel

When: Friday, Aug 7, 14:00 - 14:59 PDT

Where: LVCCW Level 1 Hall 4 1420 (Hackers.town) - [Map](#)

Description:

SpeakerBio: RabidMoosery

No BIO available



[Return to Index](#) - Add to Google

- ics [Calendar](#) file

Title: Total Recon: How We Discovered 1000s of open Agents in The Wild

Tags: Recon Village | Creator Talk/Panel

When: Saturday, Aug 8, 17:30 - 17:59 PDT

Where: LVCCW Level 1 Hall 3 1105 (Creator Stage 3) - [Map](#)

Description:

AI agents quietly created a new external attack surface: copilots, custom agents, AI cakends and various deployments that ship to the internet, often without anyone realizing they are reachable, enumerable, or over-permissive.

In this talk, we'll show how attackers can already find your agents in the wild, shedding light on the technical details that enable this kind of malicious activity, including how we used these details to find 1000s of exposed agents of different kinds. We'll follow up with explaining how to measure exposure, see the proof for obscurity failing, and understand how to detect threat-actor agent-focused recon before it turns into an impactful attack. Capping it all off by showcasing PowerPwn, a recon tool you can use to test your own exposure

Speakers: Avishai Efrat, Roey Ben Chaim

SpeakerBio: Avishai Efrat, Senior Security Researcher at Zenity

Avishai Efrat is a senior security researcher at Zenity, specializing in securing AI agents and low-code/no-code platforms. His work focuses on uncovering vulnerabilities in enterprise AI deployments, from Copilot Studio to ChatGPT and beyond - and exploring how attackers discover and exploit these weaknesses. Passionate about all aspects of security, with experience spanning web security, anti-bot protection, OSINT, blockchain, and data engineering and aim on bridging the gap between cutting-edge research and practical defense strategies. Previously presented at BSidesTLV, Black Hat USA & Europe Arsenal and SecTor.

SpeakerBio: Roey Ben Chaim, Staff Engineer at Zenity

Roey Ben Chaim is an engineer focused on AI and agent security, with a particular interest in how agentic systems fail in practice. His work centers on stress-testing agents, building benchmarks for long-horizon behavior, and developing practical defenses against risks such as prompt injection, unsafe tool use, privacy leakage, and adversarial workflows. Prior to this, he spent a decade at Microsoft building large-scale security systems. He is a co-author of SkillsBench, a benchmark on agent skills efficacy over diverse tasks, and contributes to safety and privacy tooling, including Presidio. Roey is also a speaker on agentic systems and AI security, a co-organizer of AI Tinkerers Tel Aviv, and an active participant in hackathons and builder communities, where he explores emerging systems through hands-on experimentation.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Social Gatherings/Events - Thursday - 15:00-20:59 PDT

Title: Toxic BBQ

Tags: Event

When: Thursday, Aug 6, 15:00 - 20:59 PDT

Where: Other / See Description

Description:

Join the humans of Vegas at the unofficial opener of DEF CON. This Thursday Meat-Up is in the shade of Sunset Park, a quick ride from the LVCC. We stock the larder with burgers, dogs, and fixin's. We rely on you for everything else: sides, drinks, volunteering, and donations.

With over 50 sq ft of heat, we have plenty of room on the grill for your personal creations. Contribute food and drinks, staff the grill, join supply runs, or donate to help cover cost. Everything left goes to the EFF. Be a part of what makes this cookout something to remember year after year. The only question is: What are you bringing to Toxic BBQ?

Check out toxicbbq.org , find a flyer at an NFO Node, and watch for #ToxicBBQ on the socials for the latest news.

Sunset Park, Foxtail Pavilion (Lat: 36.0636, Long: -115.1178)

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

OSINT For Good Community - Friday - 15:30-16:30 PDT

Title: Trace Labs L100: Search Party Basics

Tags: OSINT For Good Community | Creator Workshop

When: Friday, Aug 7, 15:30 - 16:30 PDT

Where: LVCCW Level 1 Hall 4 1307 (OSINT4Good Community) Stage - [Map](#)

Description:

Learn how to optimize your OSINT workflow and strengthen your performance in the Trace Labs Search Party CTF and beyond. . This session will cover core strategies, ethical guidelines, and preparation methods to help you operate confidently, efficiently, and responsibly in a real-world investigative environment. Normally offered as a paid webinar, this session is lead by a Trace Labs Director and earns a digital badge that is part of the Trace Labs webinar series.

SpeakerBio: Sarah "scba" Miller, Trace Labs

Dr. Sarah Miller is a college professor, emergency manager, cybersecurity manager, and a Director for Trace Labs.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Trace Labs L150: Case Walkthrough

Tags: OSINT For Good Community | Creator Workshop

When: Saturday, Aug 8, 10:00 - 10:59 PDT

Where: LVCCW Level 1 Hall 4 1307 (OSINT4Good Community) Stage - [Map](#)

Description:

Join us for an immersive online seminar with the Reporting Team Department Head at Trace Labs, as he walks through real missing person investigations from the Trace Labs CTFs. This session moves beyond foundational OSINT concepts and focuses on how investigations unfold in practice, from a single starting point to the development of actionable, ethically collected intelligence. Participants will follow detailed case walkthroughs drawn from Trace Labs Search Party CTF events, highlighting how analysts:

Pivot from initial clues across platforms and ecosystems Identify meaningful signals of activity Provide actionable intelligence

Normally offered as a paid webinar, this session earns a digital badge that is part of the Trace Labs webinar series.

SpeakerBio: Brent Louie, Reporting Team Lead at Trace Labs

Brent Louie is the Reporting Team Lead at Trace Labs and an Associate Director of Data Science with more than 15 years of experience in the biotechnology industry. He focuses on applying OSINT methodologies to missing persons investigations and helping transform crowdsourced research into actionable investigative leads for law enforcement.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

OSINT For Good Community - Friday - 17:30-17:59 PDT

Title: Tracelabs VM Installation Workshop

Tags: OSINT For Good Community | Creator Workshop

When: Friday, Aug 7, 17:30 - 17:59 PDT

Where: LVCCW Level 1 Hall 4 1307 (OSINT4Good Community) - [Map](#)

Description:

Need help installing or using the Trace Labs Virtual Machine? Bring your laptop and sit down for some one-on-one help from one of our volunteers.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Tracking the Trackers: How We Took Over 36 Million GPS Devices Protecting Children and Vehicles

Tags: DEF CON Official Talk | Demo | Exploit

When: Saturday, Aug 8, 11:00 - 11:59 PDT

Where: LVCCW Level 1 Hall 3 1006 (Main Track 1) - [Map](#)

Description:

We performed our research against three major GPS tracking platforms: SETracker (~10M devices, 39 brands), SinoTrack (6M+ devices), and TKSTAR/Thinkrace (20M+ devices). All three come from the same Shenzhen supply chain. All three are completely broken.

We achieved RCE on every platform, including `NT AUTHORITY\SYSTEM` on TKSTAR. From a free account with no device purchase, we can silently wiretap any child's watch, force video surveillance, steal vehicles through remote door unlock and fuel cutoff, and take over the backend servers. We filed 45 CVEs, 19 critical, 9 of them CVSS v3.1 10.0.

The worst part is the supply chain structure. 39 consumer brands in 20+ countries (Wonlex, SaveFamily, KidiWatch, Garrett, etc.) all connect to the same `myaqsh.com` server in China. Parents think they are choosing between brands. They are not. Brand diversity in this market is an illusion.

We release full PoC chains, CVE details, and a brand-to-backend mapping that shows how this industry actually works.

Speakers: Felipe Solferini, Vangelis Stykas

SpeakerBio: Felipe Solferini

Felipe is a senior penetration tester and self-proclaimed security researcher. Most of the time, he's mashing the wrong buttons, hoping for the worst but expecting the best - or just YOLOing like there's no tomorrow. Occasionally, he wonders if life is just a CTF. He has presented his research at BSides London, BSides Sofia, and BSides Vilnius.

SpeakerBio: Vangelis Stykas, Kumio

Vangelis began as a developer from Greece. Ten years ago he realized that only his dog didn't have an API, so he decided to steer his focus towards security. That led him to pursue a PhD in Web Application Security with an extra focus on machine learning. He's still actively pursuing it. He currently applies his skills as a Chief Technology Officer at Kumio, and during his free time, Vangelis is helping start-ups secure themselves on the internet and get a leg up in security terms. His love of a simplistic approach to hacking by exploiting vulnerable APIs led him to publish research regarding API controlling ships, smart locks, IP cameras, car alarms, EV chargers, and many other IoT devices. Since our lives are nowadays extremely cyber-dependent, his goal is to convince all companies to never neglect their API security as rush-to-market mentality is almost certain to lead to catastrophic security failure. He has presented his research at Black Hat USA, DEF CON, Disobey, BSides London, BSides Dublin, BSides Athens, 44Con and other security conferences, and has keynoted at BSides Prague. His most recent work on disrupting ransomware operations by hacking their web panels was featured at Black Hat USA and DEF CON 32.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Recon Village - Friday - 10:00-23:59 PDT

Title: TrackTheFugitive Contest

Tags: Recon Village | Creator Event/Activity

When: Friday, Aug 7, 10:00 - 23:59 PDT

Where: LVCCW Level 1 Hall 2 501 (Recon Village) - [Map](#)

Description:

The manhunt is on. TrackTheFugitive drops you into real, active cases where the suspects are still out there—no simulations, no canned flags. Armed with nothing but open-source intelligence, you'll chase digital breadcrumbs, unmask aliases, and surface the leads that help bring real fugitives to justice.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Recon Village - Saturday - 12:00-17:59 PDT

Title: TrackTheFugitive Contest

Tags: Recon Village | Creator Event/Activity

When: Saturday, Aug 8, 12:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 2 501 (Recon Village) - [Map](#)

Description:

The manhunt is on. TrackTheFugitive drops you into real, active cases where the suspects are still out there—no simulations, no canned flags. Armed with nothing but open-source intelligence, you'll chase digital breadcrumbs, unmask aliases, and surface the leads that help bring real fugitives to justice. Contest continues from Friday and ends Saturday at 6:00 PM.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Trajan: Cross-Platform CI/CD Security Scanner

Tags: AI | DEF CON Demo Labs | Intermediate | Cloud | Defense/Blue Team | DevOps | Offense/Red Team | Purple Team | SecOps | DEF CON Demo Labs

When: Saturday, Aug 8, 13:00 - 13:45 PDT

Where: LVCCW Level 1 Hall 3 902 (Demo Labs Track 6) - [Map](#)

Description:

For three years, Praetorian has consistently found that CI/CD pipelines are one of the fastest paths to compromise enterprise environments. A misconfigured workflow or an over-privileged service connection can provide you with credentials, cloud access, or code execution on internal infrastructure, often undetected.

We built to keep up: Gato for GitHub Actions (BH 2024), then Glato for GitLab CI (BH 2025). Both proved the approach: parse the pipeline configuration, classify triggers, gates, and danger zones, build a graph of how they connect, and surface what's actually exploitable.

The problem was that no client runs just one platform. A typical enterprise has GitHub Actions for open-source, Azure DevOps for internal deployments, and GitLab for containerized workloads. Assessing all of that meant juggling multiple tools with different output formats and coverage gaps.

Trajan folds everything we learned into a single tool spanning GitHub Actions, GitLab CI, and Azure DevOps. Each platform runs through the same phased pipeline: collect the pipeline config and the org surface, normalize it, correlate multi-step attack chains, scan against a YAML detection-rule corpus organized by attack category, and report through one unified findings format. Support for Jenkins, CircleCI, and Bitbucket is in active development.

Speakers: Rahul Saranjame, Ranganatha Rao Sridhar, Tanishq Rupaal

SpeakerBio: Rahul Saranjame

Lead Security Engineer at Praetorian focused on penetration testing, red/purple teaming, CI/CD pipeline security, and risk advisory assessments. Rahul is OSCP and CRT0 certified, holds a Master's degree in Cybersecurity from Georgia Tech, and is a core contributor to Trajan.

SpeakerBio: Ranganatha Rao Sridhar

OSCE3 certified Lead Security Engineer at Praetorian with expertise spanning product, cloud, and corporate security. Rao holds a Master's degree in Cybersecurity from Georgia Tech and is a core contributor to Trajan.

SpeakerBio: Tanishq Rupaal

Staff Offensive Security Engineer at Praetorian specializing in cloud security across AWS, GCP, and Azure. He designed the Guard Platform's cloud integration mechanism, is a core contributor to Trajan, and holds an M.S. in Cybersecurity from Georgia Tech.

Title: Trajan: Cross-Platform CI/CD Security Scanner

Tags: AI | DEF CON Demo Labs | Intermediate | Cloud | Defense/Blue Team | DevOps | Offense/Red Team | Purple Team | SecOps | DEF CON Demo Labs

When: Friday, Aug 7, 14:00 - 14:45 PDT

Where: LVCCW Level 1 Hall 3 902 (Demo Labs Track 6) - [Map](#)

Description:

For three years, Praetorian has consistently found that CI/CD pipelines are one of the fastest paths to compromise enterprise environments. A misconfigured workflow or an over-privileged service connection can provide you with credentials, cloud access, or code execution on internal infrastructure, often undetected.

We built to keep up: Gato for GitHub Actions (BH 2024), then Glato for GitLab CI (BH 2025). Both proved the approach: parse the pipeline configuration, classify triggers, gates, and danger zones, build a graph of how they connect, and surface what's actually exploitable.

The problem was that no client runs just one platform. A typical enterprise has GitHub Actions for open-source, Azure DevOps for internal deployments, and GitLab for containerized workloads. Assessing all of that meant juggling multiple tools with different output formats and coverage gaps.

Trajan folds everything we learned into a single tool spanning GitHub Actions, GitLab CI, and Azure DevOps. Each platform runs through the same phased pipeline: collect the pipeline config and the org surface, normalize it, correlate multi-step attack chains, scan against a YAML detection-rule corpus organized by attack category, and report through one unified findings format. Support for Jenkins, CircleCI, and Bitbucket is in active development.

Speakers: Rahul Saranjame, Ranganatha Rao Sridhar, Tanishq Rupaal

SpeakerBio: Rahul Saranjame

Lead Security Engineer at Praetorian focused on penetration testing, red/purple teaming, CI/CD pipeline security, and risk advisory assessments. Rahul is OSCP and CRT0 certified, holds a Master's degree in Cybersecurity from Georgia Tech, and is a core contributor to Trajan.

SpeakerBio: Ranganatha Rao Sridhar

OSCE3 certified Lead Security Engineer at Praetorian with expertise spanning product, cloud, and corporate security. Rao holds a Master's degree in Cybersecurity from Georgia Tech and is a core contributor to Trajan.

SpeakerBio: Tanishq Rupaal

Staff Offensive Security Engineer at Praetorian specializing in cloud security across AWS, GCP, and Azure. He designed the Guard Platform's cloud integration mechanism, is a core contributor to Trajan, and holds an M.S. in Cybersecurity from Georgia Tech.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Queercon Community - Saturday - 12:00-12:59 PDT

Title: Trans Meetup

Tags: Queercon Community | Creator Event/Activity

When: Saturday, Aug 8, 12:00 - 12:59 PDT

Where: LVCCW Level 3 W325 (QueerCon Lounge) - [Map](#)

Description:



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Queercon Community - Friday - 11:00-11:59 PDT

Title: Trans Townhall

Tags: Queercon Community | Creator Event/Activity

When: Friday, Aug 7, 11:00 - 11:59 PDT

Where: LVCCW Level 3 W325 (QueerCon Lounge) - [Map](#)

Description:

Join us for the Trans Town Hall to find connections, discuss challenges facing the trans community, and engage in conversations critical to the community.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Transformers: Dark Side of the Type - Weaponizing the Conversion Layer

Tags: DEF CON Official Talk | Demo | Exploit

When: Saturday, Aug 8, 13:30 - 14:30 PDT

Where: LVCCW Level 1 Hall 3 904 (Main Track 4) - [Map](#)

Description:

In 2017, our DEF CON talk "Friday the 13th: JSON Attacks" forced the industry to confront Insecure Deserialization. Developers responded by hardening the configurations of parsers and serializers. But it created a dangerous blind spot. Developers and security reviewers now assume that simpler code patterns, those that do not involve parsers, are inherently safe. We demonstrate that they are not. This talk moves the focus away from the serialization format entirely and targets the transformation layer: the code that turns a simple string into a complex object. We expose "Insecure String Transformers": mechanisms that silently resolve types, trigger complex logic, and instantiate objects during what looks like a safe string conversion. This overlooked attack surface remains invisible to the tools and reviews focused on the parser-level bugs from 2017. We dissect specific CVEs where string-to-object conversion was the root cause of RCE. We release new gadget chains targeting popular .NET libraries and present a methodology for hunting dangerous conversion patterns across any codebase. The goal is to redefine how the industry classifies this vulnerability: it is not "Insecure Deserialization" - it is Insecure Transformation, and it may be hiding in your application even if it does not use any serialization library.

Alvaro Muñoz & Oleksandr Mirosh, "Friday the 13th: JSON Attacks" - Black Hat USA 2017

<https://www.blackhat.com/docs/us-17/thursday/us-17-Munoz-Friday-The-13th-JSON-Attacks-wp.pdf> Alvaro Muñoz &

Oleksandr Mirosh, "Room for Escape: Scribbling Outside the Lines of Template Security" - Black Hat USA 2020

<https://i.blackhat.com/USA-20/Wednesday/us-20-Munoz-Room-For-Escape-Scribbling-Outside-The-Lines-Of-Template-Security->

SpeakerBio: Oleksandr Mirosh, OpenText Fortify

Oleksandr Mirosh is a Security Researcher on the Fortify Software Security Research team at OpenText, where he focuses on investigating emerging threats and developing detection and remediation rules for enterprise software. With over 18 years of experience in computer security, specializing in vulnerability research, reverse engineering, and penetration testing, his work centers on flaws in JNDI, authentication protocols, data serialization, and transformation logic across Java and .NET ecosystems. His research has led to the discovery of numerous CVEs in widely deployed enterprise applications and framework libraries. A frequent speaker at Black Hat USA and DEF CON, he has also presented at other security conferences like OWASP Global AppSec and BSidesLV.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Travel Security: Viewing Risks Through the Eyes of a Hacker

Tags: Physical Security Village | Creator Talk/Panel

When: Sunday, Aug 9, 12:00 - 12:59 PDT

Where: LVCCW Level 1 Hall 3 1104 (Creator Stage 4) - [Map](#)

Description:

Drawing from real-world examples, covert entry, red team, and social engineering engagements, Tim Roberts and Brent White walk through how everyday travel habits can expose individuals and organizations to unnecessary risk. From airports and hotels to conferences, rideshares, restaurants, and more...we'll look at how attackers identify opportunities and observations most travelers never think about.

This talk focuses on practical awareness rather than paranoia! We'll discuss common hotel vulnerabilities, social engineering tactics used against staff and travelers, and how small mistakes can lead to physical, identity theft, digital, or information compromise. Attendees should leave with realistic, affordable techniques they can immediately apply to improve situational awareness and protect their privacy. The goal isn't to be paranoid; it's to better understand how attackers think and make yourself a harder target!

Speakers: Tim Roberts, Brent White

SpeakerBio: Tim Roberts, Sr. Principal Security Consultant and Red Team Operator at Dark Wolf

Tim Roberts is a Sr. Principal Security Consultant and Red Team Operator with Dark Wolf, specializing in covert entry, OSINT, social engineering, and adversary-driven Red Team operations. His work includes physical and electronic access control bypassing, physical site assessments, surveillance, wireless and network penetration testing, drone hacking, web application security, and full-spectrum offensive security testing across government and commercial environments.

With more than two decades of experience across private industry and government sectors, Tim has conducted assessments against highly secured facilities and critical infrastructure designed to emulate real-world adversaries. He is a co-author of the popular ACCESS LOGS series with Covert Instruments and has worked alongside law enforcement agencies supporting special operations cyber initiatives.

Tim has been featured on Microsoft's Roadtrip Nation, Profiling Evil with Mike King, Hak5, Security Weekly, and BBC News. His work has also been highlighted by IDG Enterprise's CSO Online and Help Net Security for expertise in social engineering, adversary methodology, and security awareness.

Through WeHackPeople.com, Tim continues contributing to the security industry and InfoSec community by sharing real-world tradecraft, lessons learned, and both traditional and non-traditional techniques used in commercial and government operations.

SpeakerBio: Brent White, Sr. Principal Security Consultant and Red Team Operator at Dark Wolf

Brent White is a Sr. Principal Security Consultant and Red Team Operator with Dark Wolf, specializing in covert entry, OSINT, social engineering, and adversary-driven Red Team operations. His work includes physical and electronic access control bypassing, physical site assessments, surveillance, wireless and network penetration testing, web application security, and full-spectrum offensive security testing across government and commercial environments.

With his experience across private industry and government sectors, Brent has conducted assessments against highly secured facilities and critical infrastructure designed to emulate real-world adversaries. He is a co-author of the popular ACCESS LOGS series with Covert Instruments and has worked alongside law enforcement agencies supporting special operations cyber

initiatives.

Brent contributed to drone hacking methodology development for the Defense Innovation Unit's Blue sUAS initiative and helps lead Aerospace Village Drone Hacking operations at DEF CON. He has also been featured on Microsoft's Roadtrip Nation, ProfilingEvil with Mike King, Hak5, Security Weekly, and BBC News, while his work has been highlighted by IDG Enterprise's CSO Online and Help Net Security.

Through WeHackPeople.com, Brent continues contributing to the security industry and InfoSec community by sharing real-world tradecraft, lessons learned, and both traditional and non-traditional techniques used in commercial and government operations.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Triage vs. Reality: Mobile Security Findings in Bug Bounty

Tags: Mobile Hacking Community | Creator Talk/Panel

When: Saturday, Aug 8, 12:30 - 12:59 PDT

Where: LVCCW Level 1 Hall 4 1422 (Mobile Hacking Community) - [Map](#)

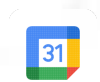
Description:

Mobile bug bounty has matured significantly, but the way mobile vulnerabilities are evaluated has not kept pace. Researchers frequently encounter findings that don't fit neatly into traditional scoring frameworks, rely on application-specific threat models, or require multiple seemingly low-impact issues to demonstrate meaningful risk. The result is inconsistent triage, misunderstood impact, and unnecessary friction between researchers and programs.

This talk explores why mobile security findings are uniquely challenging to assess and where current bug bounty processes fall short. We'll examine common pitfalls in mobile triage, discuss the limitations of applying generic scoring systems such as CVSS to mobile vulnerabilities, and look at real-world examples where technical severity and triage outcomes diverged.

SpeakerBio: fr4vian

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Trust Amplification in Enterprise AI Systems – Microsoft CoPilot Case Studies Enabling AI-Assisted Influence Operations

Tags: AI Village | Creator Talk/Panel

When: Saturday, Aug 8, 16:30 - 16:59 PDT

Where: LVCCW Level 1 Hall 3 801 (Creator Stage 1) - [Map](#)

Description:

Enterprise AI assistants such as Microsoft Copilot are rapidly becoming embedded in business workflows, granting them unprecedented influence over how users discover information, make decisions, and interact with organizational data. While much of the current security discussion focuses on prompt injection itself, the larger risk may be what happens after that influence occurs.

This talk discusses the concept of Trust Amplification, a model in which attacker-controlled content gains credibility as it is transformed, contextualized, and redistributed by enterprise AI systems. Through real-world Microsoft Copilot case studies, we demonstrate how indirect prompt injection can influence document conversion workflows, persist through shared collaboration sessions, and transform traditional device code phishing into trusted AI-generated authentication guidance.

Rather than introducing entirely new attack classes, enterprise AI systems can act as force multipliers for existing social engineering techniques by presenting attacker influence through trusted enterprise platforms and workflows. We conclude by introducing Locusta, an open-source enterprise AI collaboration and propagation toolkit developed to help red teams and defenders model these emerging attack paths and better understand how influence can spread through AI-assisted environments.

SpeakerBio: Tobias Diehl

Tobias Diehl is a Senior Offensive Security Engineer, security researcher, and Microsoft 2025 Most Valuable Researcher (MVR) specializing in offensive security, enterprise AI, bug bounty research, and adversary emulation. His work focuses on identifying overlooked attack paths where web applications, AI systems, and desktop software intersect, helping organizations understand how seemingly low-risk vulnerabilities can become high-impact security issues. Tobias leads offensive security assessments, conducts purple team exercises, and performs research into emerging attack techniques affecting enterprise environments. His work has resulted in multiple security findings impacting Microsoft technologies, including Power Platform, CoPilot and other AI-driven applications. A returning DEF CON speaker, Tobias is passionate about sharing practical research that helps both security researchers and defenders better understand modern attack chains. His presentations emphasize real-world case studies, responsible disclosure, and actionable defensive guidance for securing the next generation of AI-enabled enterprise systems.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Trust Fall: How Agentic AI Inherits Your Cloud's Worst IAM Habits

Tags: Cloud Village | Creator Talk/Panel

When: Friday, Aug 7, 16:50 - 17:30 PDT

Where: LVCCW Level 3 W313 (Cloud Village Talks) - [Map](#)

Description:

Cloud IAM was designed for two principals: humans and machines. In 2026, a third has arrived: the autonomous AI agent and it plays by neither rule book. AWS Bedrock Agents, LangChain-based orchestrators, and multi-agent pipelines are being deployed with execution roles scoped to whatever the deploying engineer thought was "good enough," inheriting the same over-privileged IAM patterns that have plagued cloud environments for a decade. The difference: agents don't just misuse permissions accidentally. When adversarial manipulations are done, they weaponize them with precision.

This talk dissects the threat model of agentic AI systems from an attacker's perspective with a clear-eyed look at how autonomous agents become cloud privilege escalation engines. Drawing from the OWASP Top 10 for Agentic Applications 2026, MITRE ATLAS, and real-world research including Sonrai Security's AgentCore privilege escalation path and Unit 42's confirmation of autonomous AI-driven cloud attacks, the talk walks through a complete attack chain: indirect prompt injection against an agent's context window → tool misuse via over-privileged Lambda execution roles → IAM policy modification → persistent backdoor creation — all without a single stolen credential.

Attendees will leave with a structured threat model mapped to MITRE ATLAS tactics, a dissection of what AWS CloudTrail catches versus what it silently misses during agent-driven attacks, a breakdown of the three OWASP agentic risks most directly applicable to AWS environments (Goal Hijack, Tool Misuse, Identity & Privilege Abuse), and concrete defensive controls including agent-scoped least-privilege IAM, Bedrock Guardrails limitations practitioners need to know, and human-in-the-loop architectural patterns.

Speakers: Aravind Sreekanth Pallavoor, Sadhana Sainarayanan

SpeakerBio: Aravind Sreekanth Pallavoor

Aravind Pallavoor is a cybersecurity practitioner with over five years of hands-on experience spanning application security, cloud security engineering, and offensive security research. He holds CISSP, CEH (v11), and AWS Certified Security – Specialty (SCS-C02) certifications alongside a Master of Science in Cybersecurity, Technology and Policy from The University of Texas at Dallas, where he graduated with a 3.82 GPA.

His offensive security background includes web application and API penetration testing, mobile application security, AI chatbot security assessments — including prompt injection and training data poisoning research — and cloud infrastructure security across AWS environments. He has conducted security assessments for global financial institutions and enterprise SaaS organizations, applying frameworks including OWASP, CVSS, MITRE ATT&CK, NIST, PCI DSS, and CIS Foundations.

On the cloud side, Aravind has directly architected and audited IAM environments, deployed and red-teamed compliance automation pipelines, and operationalized AWS Config, Secrets Manager, and CI/CD pipeline security at scale. His research interest at the intersection of agentic AI and cloud identity — the subject of this talk — grew directly from real-world experience testing AI systems for adversarial manipulation and observing how autonomous tool use exposes cloud IAM to a new class of attack surface.

"Trust Fall" represents his synthesis of those two worlds: offensive AI security research applied to the cloud IAM threat model, grounded in published vulnerability research, OWASP's Agentic Top 10 for 2026, and MITRE ATLAS — and delivered without a lab, because the threat model speaks for itself.

Additional Speaker Bio: Sadhana Sainarayanan is an AI and machine learning practitioner with deep expertise in autonomous pipeline design, event-driven system architecture, MLOps, and cloud-native AI deployment across GCP and Azure environments. She holds a Google Cloud Certified Professional Machine Learning Engineer certification and a Microsoft Certified Azure AI Engineer Associate certification, alongside dual Master's degrees from Carnegie Mellon University. Her research interests span the security implications of agentic AI systems, NLP pipeline trust boundaries, and the input-validation gaps that emerge when autonomous systems process external data at scale. For this talk, she brings the AI builder's perspective to the cloud identity threat model.

Additional Speaker LinkedIn: <http://www.linkedin.com/in/sadhana-sainarayanan>

SpeakerBio: Sadhana Sainarayanan

Sadhana Sainarayanan is a Cloud Platform Security Analyst with experience across SAP BTP security operations, ML pipeline productionization and AI systems. She holds dual master's degrees from Carnegie Mellon University in Engineering and Technology Innovation Management, and Civil and Environmental Engineering. Her independent projects span instrumentation for AI systems, focused on the gap between what agents report doing and what they actually do, execution auditing, and behavioral divergence detection.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Red Team Village - Friday - 16:00-16:59 PDT

Title: Trust Me, Bro: A field guide to Windows Authenticode Abuse

Tags: Red Team Village | Misc

When: Friday, Aug 7, 16:00 - 16:59 PDT

Where: LVCCW Level 1 Hall 1 309 (Red Team Village) Workshop Stage 1 - [Map](#)

Description:

This talk breaks down how Windows code signing fails. You learn why signed binaries still bypass trust checks and why users click through warnings. The session walks through signature abuse, metadata cloning, and SIP hijacking with live demos and explain the pros and cons. You see how attackers make malware appear trusted by the OS and trick the user.

You also see how these techniques can get chained together through with the tool "TrustMeBro".

SpeakerBio: Fagan Afandiyev

Fagan Afandiyev is a cybersecurity student and offensive security engineer based in Tampa, Florida. His work focuses on Active Directory attacks and Windows internals. He works as an Offensive Security Intern at White Knight Labs and contributes to open source tooling used in real penetration tests.

He holds multiple industry certifications, including CPTS, CAPE, CRT0, ARTO, CBBH, and CompTIA Security+. He competes regularly and has earned first place finishes at DEF CON Adversary Village, BSides Tampa, Social Engineering TempleLabs, and NCAE Cyber Games. He previously served as President of the Whitehatters Computer Security Club at the University of South Florida teaching people about cybersecurity.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Trust No History: Why Every "Remembered" Interaction is a Potential Backdoor

Tags: Intermediate | AppSec Village | Creator Talk/Panel

When: Friday, Aug 7, 17:30 - 17:59 PDT

Where: LVCCW Level 1 Hall 2 604 (Appsec Village) Main Stage - [Map](#)

Description:

As AI transitions from stateless tools to autonomous agents, the context window has become the primary attack surface. By giving agents the ability to remember, summarize, and collaborate, we have created a machine that can be gaslit. This session moves beyond transient prompt injections into the realm of persistent memory corruption. We explore how an adversary can rewrite an agent's history, bias its knowledge base, and plant sleeper instructions that trigger long after the initial interaction. We will dissect the systematic subversion of the agentic memory stack and demonstrate why developers must stop treating agent memory as a passive data store and start defending it as the engine of the agent's survival

Speakers: Barno Kaharova, Rico Komenda

SpeakerBio: Barno Kaharova

Barno is a consultant and researcher specializing in AI security, data engineering, and ML security. She works at the intersection of offensive and defensive AI security, developing methodologies to protect AI systems from adversarial threats across the full stack from data pipelines and ML models to LLM-powered applications and autonomous agents. As an AI security trainer, Barno designs and delivers hands-on programs covering AI red teaming, prompt injection, adversarial ML, RAG and vector database security, and the OWASP Top 10 for LLM and Agentic AI. Her approach is practitioner-first: participants attack and defend real-world AI systems, leaving with techniques they can apply immediately. She is actively involved in AI governance and evaluation efforts at the national level and regularly contributes to the AI security community through speaking engagements, publications, and conference submissions, bridging rapid AI adoption with the need for robust, field-tested defenses.

SpeakerBio: Rico Komenda

Rico Komenda is a security engineer and researcher specializing in application security, cloud security, and AI security. He started as a software developer, moved into security engineering, and now focuses on the attack surface created by AI-integrated systems and secure agentic development.

He is Co-Lead of the OWASP AI Security Verification Standard (AISVS) and a core contributor to multiple OWASP GenAI security projects. Rico has spoken at NDC Security, OWASP Global AppSec EU, OWASP LASCON, WeAreDevelopers World Congress, DefCamp, and others.

He got into this field the way a lot of hackers do: writing scripts for video games as a teenager, getting curious about how systems break, and never stopping.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Trust the Basics, But Know Their Limits: Where Standard Cybersecurity Advice Falls Short

Tags: Crypto & Privacy Village | Creator Talk/Panel

When: Friday, Aug 7, 13:00 - 13:30 PDT

Where: LVCCW Level 1 Hall 3 1104 (Creator Stage 4) - [Map](#)

Description:

Those cybersecurity tips you've heard over and over again are still our best defense against attackers, but following them doesn't actually protect you from everything.

In 2026, we know that freezing your credit won't protect you from most scams, and that even the strongest password manager can't save a compromised device. So what actually works, and where does it fall short?

The advice is good. The gaps are real. Come learn both.

SpeakerBio: Yael Grauer

Yael is an investigative tech reporter covering privacy and security, digital freedom, hacking, and mass surveillance. She contributed to a Pulitzer Prize-winning AP investigative package on surveillance, and spent six years at a media nonprofit managing cybersecurity tools and programs that reached hundreds of thousands of users. She holds a CIPP-US certification and has completed way too many cybersecurity and source protection programs.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Trust the Cloud Pipeline, Lose the Kingdom

Tags: Cloud Village | Creator Talk/Panel

When: Saturday, Aug 8, 11:20 - 11:59 PDT

Where: LVCCW Level 3 W313 (Cloud Village Talks) - [Map](#)

Description:

In 2020, SolarWinds showed the industry what it looks like when an attacker owns a build pipeline. In 2021, Codecov did it again. CircleCI in 2023. Each incident surfaced the same pattern. Cloud CI/CD systems sit at the center of a trust graph most organizations have never actually mapped, and compromising them grants access to everything downstream: source code, cloud infrastructure, production artifacts, customer data, and every third party platform the organization stores credentials for. Detection remains largely absent.

Five years after SolarWinds, red teams still rarely operate meaningfully against cloud native CI/CD. Most offensive security programs treat pipelines as infrastructure they inherit rather than terrain they fight over. Defenders build detection around endpoints and identities they recognize, while ephemeral build agents with elevated cloud credentials run continuously and unmonitored.

This talk presents a full cloud native CI/CD attack chain drawn from red team engagements across multiple enterprise cloud environments. The chain starts at a low privilege developer identity. Pull request poisoning, in both direct and indirect variants, exfiltrates temporary AWS credentials from the build agent. A scheduled Lambda function then relays fresh credentials before each expiry, providing durable serverless persistence with no endpoints, no implants, and no signals a traditional detection stack watches for. IAM role trust chain abuse escalates the compromised build identity into broad cloud access spanning multiple accounts. Finally, Secrets Manager extends the attack beyond AWS. The credentials stored inside grant organization admin access to the code hosting platform, administrative control of the CI platform itself, access to customer data warehouses, and access to every SaaS and third party system the organization depends on.

Attendees will walk away with a concrete mental model of how cloud native CI/CD fails under adversarial pressure, a specific set of detection rules that would have caught each stage (deployable against CloudTrail and CI logs most organizations already collect), and structural guidance for where trust boundaries need to exist between build infrastructure and production.

Intermediate audience. Familiarity with AWS IAM and general CI/CD concepts is helpful; the relevant cloud mechanics will be explained as needed.

SpeakerBio: Shane Young

Shane Young is an offensive security operator and program builder with over 15 years in the field. His career spans consulting across financial services, hardware, and SaaS; building out an IoT security practice at a major security consultancy; leading red team operations against cloud native product companies; and pioneering AI/ML red teaming for deployed enterprise AI features. He is the creator of Brutepay, a public open source offensive security tool. He builds offensive security programs from scratch, runs red team operations end to end, and still carries significant technical IC workload because he thinks that is how security leaders stay sharp. He has been hacking since he was a teenager, and it still has not gotten old.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Trust the Pipeline, Lose the Kingdom: Hands-On Cloud Native CI/CD Red Team

Tags: Red Team Village | Misc

When: Friday, Aug 7, 15:00 - 15:59 PDT

Where: LVCCW Level 1 Hall 1 309 (Red Team Village) Workshop Stage 1 - [Map](#)

Description:

Cloud native CI/CD pipelines are the soft underbelly of modern enterprise security. SolarWinds in 2020, Codecov in 2021, CircleCI in 2023 set the template, and the pattern has only accelerated: tj-actions compromised 23,000 repositories in March 2025, GhostAction exfiltrated 3,325 secrets in September 2025, TeamPCP turned Trivy and Checkmarx GitHub Actions into credential stealers in March 2026. Most red teams still do not operate meaningfully against cloud CI/CD, and most detection stacks still do not watch it. The terrain runs in the gap between endpoint detection and cloud API monitoring, and it remains one of the highest leverage, least contested surfaces in the enterprise.

This workshop walks a full cloud native CI/CD attack chain drawn from multiple red team engagements: pull request poisoning via `pull_request_target`, OIDC-to-STS credential exfiltration from the build runner, force-merging a PR through a GitHub admin PAT pulled from Secrets Manager, Lambda and EventBridge persistence that never leaves the cloud, IAM trust chain abuse that escalates a low privilege build identity into broad cloud access, and Secrets Manager as the pivot out of AWS into code hosting, the CI platform, and every SaaS the organization depends on.

The paired 60 minute Tactic is hands-on, not demonstration. Each of 10 to 15 attendees forks a public demo repo and opens their own PR against it. The vulnerable `pull_request_target` workflow fires automatically and dumps live STS credentials to the workflow log. Attendees read the credentials from their own PR's Actions page, paste them into their own terminal, pull a GitHub admin PAT from Secrets Manager, and force-merge their own PR through the stolen token with no human reviewer in the loop. Every attendee watches their own PR flip from Open to Merged using a credential that did not exist until they opened the PR. The OIDC-trusted role is scoped to `GetSecretValue` on one secret, so attendee actions have zero AWS blast radius. The speaker then demonstrates the persistence, IAM trust chain, and pivot stages on the projector, and attendees leave with a public Terraform bundle to run the full chain end to end against their own AWS account at home, plus a set of detection signals deployable against CloudTrail and CI logs their organizations already collect.

SpeakerBio: Shane Young

Shane Young is an offensive security operator and program builder with over 15 years in the field. His career spans consulting across financial services, hardware, and SaaS; building out an IoT security practice at a major security consultancy; leading red team operations against cloud native product companies; and pioneering AI/ML red teaming for deployed enterprise AI features. He is the creator of Brutepay, a public open source offensive security tool. He builds offensive security programs from scratch, runs red team operations end to end, and still carries significant technical IC workload because he thinks that is how security leaders stay sharp. He has been hacking since he was a teenager, and it still has not gotten old.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Red Team Village - Friday - 11:00-11:59 PDT

Title: Trusted Launcher, Untrusted Code: Weaponizing AppLaunch.exe to bypass SmartScreen and AppLocker

Tags: Red Team Village | Misc

When: Friday, Aug 7, 11:00 - 11:59 PDT

Where: LVCCW Level 1 Hall 1 309 (Red Team Village) Workshop Stage 1 - [Map](#)

Description:

AppLocker, SmartScreen, and Windows Defender Application Control (WDAC) are the standards for securing enterprise endpoints through application whitelisting. A little-known Microsoft tool, AppLaunch, which has little to no research done, can be abused to bypass these common defenses to achieve initial access and persistence.

This talk will present a new ClickOnce deployment method using partial trust apps that launch from AppLaunch, a signed Microsoft executable that launches partial trust ClickOnce apps. This technique functions using unsigned code within default AppLocker environments with DLL signing enabled. This presentation will take a dive into exploiting and describing this novel technique.

This presentation also includes multiple novel techniques used to break out of a .NET CAS (Code Access Security) sandbox. To showcase real-world exploitability, multiple demonstrations and techniques will be displayed. This talk will explore the faulty trust model that enables a new initial access and LOLBAS (Living off the Land Binaries and Scripts) method.

A tool is provided to assist in the creation of deployments that abuse this new method. Furthermore, I will cover the IOC's left behind, and how to block and detect this attack.

SpeakerBio: Nathan Sawyer, Independent Researcher

Nathan Sawyer is a junior studying Cybersecurity at the University of Idaho. He has obtained HTB CDSA and CPTS. He enjoys skiing, snowboarding, hockey, and lacrosse.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Tu foco IoT nunca tuvo modelo de amenazas

Tags: La Villa Community | Creator Talk/Panel

When: Sunday, Aug 9, 10:00 - 10:30 PDT

Where: LVCCW Level 1 Hall 4 1416 (La Villa Community) Main Stage - [Map](#)

Description:

Compraste una foco IoT. La conectaste a tu WiFi. Le pusiste una contraseña.

¿Quién más le puede mandar órdenes? ¿Quién verifica que el firmware que descarga es legítimo?

En esta charla cuento la auditoría completa de Magic Home — la app de Zengge instalada en

bombillas, tiras LED y switches que se venden bajo una docena de marcas blancas. No

vengo a enumerar bugs. Vengo a mostrar tres preguntas básicas que el ecosistema entero —

móvil, nube y radio — no puede responder una sola raíz: nunca hubo modelo de amenazas en el ciclo del producto.

Uso firmware ya publicado en internet, scripts caseros y un decompilador. Cero hardware

comprado. Una demo grabada de por qué nada detendría a un atacante. Una demo en vivo de

cuánto se puede ver del fleet sin tocar a nadie más.

SpeakerBio: Andres Sabas, Electronic Cats

Co fundador de Electronic Cats, promotor del hardware abierto, co creador de productos de seguridad como HunterCat, Minino y BomberCat

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Turning Keys and Opening Doors: Leveraging AI Hype to Hack Everything

Tags: Red Team Village | Misc

When: Saturday, Aug 8, 14:00 - 14:59 PDT

Where: LVCCW Level 1 Hall 1 309 (Red Team Village) Workshop Stage 1 - [Map](#)

Description:

Abstract I've been Red Teaming for over five years now, and in that time I've led or been involved in more than a dozen Red Team engagements where my team has successfully (or semi-successfully) reached objective. I'm not an elite hacker. I've learned some cool tactics and techniques through public research and have pieced them together with my team to covertly pivot through networks and access sensitive data. I've decided that, while I'm not an elite hacker, I am really good at turning keys and opening doors.

In this talk I'd like to discuss how I led my company's first AI Red Team operation, not just by jailbreaking and prompt injecting LLMs; But by backdooring legitimate AI models, socially engineering data scientists, attacking ML pipelines, and abusing new AI technology to exfiltrate sensitive training data and proprietary models.

Outline Discussion of AI operation planning and offensive research - starting with zero AI knowledge

Identification of novel GCP attack + pairing it with convincing social engineering pretexts

How we sent 3000+ phish in under 10 minutes, tech stack and relevant automation

Demo of the novel GCP attack which leads to account takeover

Discussion of how the entire attack happens in the ATTACKER's GCP environment, leaving defenders blind

Automated post-exploitation for persistence and dealing with short lived keys from the GCP attack

Pivoting to AI related loot

Collaboration with Google to mitigate the risk for ALL GCP customers

Additional offensive GCP AI attacks like attacking model training pipelines with malicious containers and backdooring legitimate public models

In this talk I plan to publicly disclose a novel GCP attack path that enabled my team to take over GCP accounts and projects. This is an open vulnerability in Google's Vulnerability Reporting Programm sitting at P1.

SpeakerBio: Will Alexander

Senior Manager - Red Team @ Palo Alto Networks 2 years of Purple Teaming 5+ years of Red Teaming <1 year of Management

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Turning Recon Coverage into Bug Bounty Signal

Tags: Bug Bounty Village | Creator Talk/Panel

When: Saturday, Aug 8, 10:00 - 10:45 PDT

Where: LVCCW Level 2 W206-207 (Bug Bounty Village) - [Map](#)

Description:

Bug bounty programs increasingly face a paradox. While organisations have more tooling than ever to enumerate their internet-facing services, yet both hackers and program owners still miss real, reportable vulnerabilities, especially in volatile, sprawling environments. As the time to discover and exploit vulnerabilities collapses, effective asset discovery has become more urgent. This talk shares outcomes from the CrowdRecon initiative: a recon-first approach designed to demonstrate the true value of hacker reconnaissance, over and above what scanners and attack surface management solutions typically deliver. We'll show how recon, when treated as a disciplined, repeatable workflow (not "spray-and-pray" enumeration), produces measurable advantages across the vulnerability lifecycle: - Pre-vulnerability discovery: uncovering unknown, shifting, or mis-modeled assets (and the fragile trust assumptions around them). - At-vulnerability discovery: increasing the odds of finding real exploitable paths by mapping relationships, auth boundaries, and "hidden surfaces" that scanners miss. - Post-vulnerability context: accelerating impact validation and exploitability assessment with recon artifacts that explain why this system matters and how it is reachable. Outputs: - Examples of coverage gained (new endpoints, subdomains, environments, and trust paths) that were not represented in conventional inventories. - Patterns of high-signal recon artifacts that correlate with meaningful bounty submissions. - Common failure modes of scanner-only and AI-only approaches, and how recon closes the gap. The goal is to give bug bounty practitioners, hackers, program managers, and triage teams, an actionable mental model and set of techniques for building a "flywheel" that improves discovery without compromising ethics. An open Q&A session at the end aims to drive discussion on opening recon information to all hunters. Democratised recon.

SpeakerBio: Radu Stefan Voloaga, Senior Product Manager, Intigriti

Radu Voloaga is a Senior Product Manager at Intigriti, working at the intersection of customers, security researchers, and crowdsourced security programs. He collaborates closely with organizations and the hacker community to understand what drives high-signal discoveries, and how reconnaissance, asset discovery, and hacker behavior translate into actionable security intelligence. Radu leads the development of Crowd Recon, an initiative focused on making the activity that happens between vulnerability reports measurable and actionable. By transforming researcher-driven reconnaissance into structured signals, Crowd Recon helps surface attack surface blind spots that traditional approaches often miss while complementing scanners, AI, and attack surface management tooling. He also spends an unreasonable amount of time wondering who created a particular internet-facing asset, why it still exists, and whether anyone remembers owning it.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Two NICs, Zero Trust: Pulling Apart a PAC Buried in Critical Infrastructure

Tags: ICS Village | Creator Talk/Panel

When: Sunday, Aug 9, 12:30 - 12:59 PDT

Where: LVCCW Level 1 Hall 3 801 (Creator Stage 1) - [Map](#)

Description:

Imagine you get called up by a large CNI operator - "We have these devices, they're all over our outstations and they sit between our most critical OT trust zones", would you want to take a look? We did what any curious gremlins would do: we bought the hardware, built a bench, and started pulling at every thread. This talk tells the investigation as it actually happened, starting with architecture and documentation, moving through firmware analysis and protocol dissection, and ending with full pwnage at the firmware and application layers. Along the way we found a security model that felt frozen in the 2010s: weak trust boundaries, unauthenticated reconfiguration paths, and cryptographic protections as strong as wet cardboard. The point of the talk is not "bench testing is cool."; It's how to take a standard CNI concern into a hardware-led investigation that uncovers flaws a network-only pen test will miss. Attendees will leave with a practical workflow for assessing OT devices at scale, a mental model for deciding when to go from docs to firmware to hands-on testing, and a clear picture of how apparently boring PACs can become high-value footholds inside critical infrastructure. Nation-state level firmware backdoors and research artefacts will be released alongside this talk.

Speakers: Adam Bromiley, Sam Thom

SpeakerBio: Adam Bromiley, Pen Test Partners

Adam is a security consultant at Pen Test Partners who specialises in industrial control systems and embedded hardware security. He's worked on everything safety-critical: from high-speed rail to aircraft, power stations, and gas distribution. His embedded work has seen him break driverless cars, slot machines, and drones and has led to the responsible

disclosure of numerous vulnerabilities in industrial controllers. Adam enjoys hands-on and boots-on-the-ground testing, reverse engineering, and providing practical security advice for complex real-world systems.

SpeakerBio: Sam Thom

Sam is a security consultant at Pen Test Partners who focuses on the weird stuff - hardware, IoT and Operational Technology. He's poked and prodded Industrial and embedded systems across various industries like automotive, IoT, IIoT, chemical, water, power, gas, manufacturing and his favourite of all - the alcohol industry. Sam enjoys tearing down operational systems on the bench almost as much as owning them in the field.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: UAiRT: Over The Air UART

Tags: IoT Village | Creator Talk/Panel

When: Saturday, Aug 8, 14:30 - 15:15 PDT

Where: LVCCW Level 1 Hall 3 1105 (Creator Stage 3) - [Map](#)

Description:

The industry relies heavily on zero-trust architectures, TLS tunneling, and WAN monitoring to secure ISP edge gateways. But what happens when the compromise is soldered directly to the motherboard? Introducing Project UAiRT (UART Air interface & Remote Transmission). This presentation explores a devastating supply-chain and physical access attack utilizing a tiny \$5 ESP32-C3 microcontroller implanted inside a production grade ISP router. By hardwiring the ESP32 directly to the router's internal power rails and UART debug headers, we establish an undetectable, out-of-band Command & Control (C2) bridge that completely bypasses the router's internal firewalls and the ISP's network monitoring. Project UAiRT is not a dumb serial bridge, it is an intelligent parasite. In this talk, we will demonstrate how to weaponize the ESP32's additional GPIO pins to create a "state-aware" implant. By wiring these pins to the router's internal status LEDs and reset lines, the UAiRT module actively monitors the router's hardware state. Attendees will see a live demonstration of the ESP32 detecting a system reboot via LED voltage changes, calculating the exact microsecond delay, and autonomously firing a carriage return to interrupt the bootloaders. From this stealthy vantage point, we will use covert wireless channels (BLE, hidden Wi-Fi, and ESP-NOW) to remotely trigger filesystem modifications, drop persistent root shells, and hijack the ISP's TR-069 management daemon, proving that software security means nothing if the supply chain is compromised by a piece of silicon the size of a thumbnail.

Speakers: Metehan Arslan, Samet Berk Simsek

SpeakerBio: Metehan Arslan

No BIO available

SpeakerBio: Samet Berk Simsek

Samet Berk Şimşek is a Turknet Cyber Security Specialist & Web3 Developer

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Contests - Friday - 16:00-17:59 PDT

Title: Um, ACKtually

Tags: Um, ACKtually | Contest

When: Friday, Aug 7, 16:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 100 (Contest Stage) - [Map](#)

Description:

Um, ACKtually is returning for it's 2nd year at DEF CON 34! If you've ever seen the popular Dropout TV game-show "Um, Actually", then you know exactly who we stole this idea from.

Three contestants will compete for the Pedantic Hacker crown, providing corrections for (just barely) incorrect statements given by the hosts about everything from general technology, cyber security, and overall nerd culture. We will chum the waters of the question pool with red herrings and wrong turns while the sharks circle to be the first to answer "WELL, UM ACKTUALLY...".

Um, ACKtually celebrates everything hacker culture was built on. Community knowledge share, deep subject matter expertise of niche topics, and an almost orgasmic feeling of superiority at correcting someone else's mistakes, live and in public.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Nix Vegas Community - Sunday - 13:30-14:30 PDT

Title: Unconference

Tags: Nix Vegas Community | Creator Event/Activity

When: Sunday, Aug 9, 13:30 - 14:30 PDT

Where: LVCCW Level 1 Hall 4 1310 (Nix Vegas Community) - [Map](#)

Description:

Come and chill in the Nix Vegas space for the Unconference.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Car Hacking Village - Sunday - 10:30-10:59 PDT

Title: Unlocking Vehicles by Brute-Forcing Rolling Code Systems

Tags: Car Hacking Village | Creator Talk/Panel

When: Sunday, Aug 9, 10:30 - 10:59 PDT

Where: LVCCW Level 1 Hall 3 801 (Creator Stage 1) - [Map](#)

Description:

Many vehicles worldwide rely on a popular aftermarket rolling code system that has long been trusted to protect against key fob cloning and unauthorized access. This talk unveils the reverse engineering journey that uncovered the protocol's frame format, cryptographic design, and previously undocumented weaknesses. By combining a rollback vulnerability with a practical rolling code brute force attack, we demonstrate how an attacker can recover valid codes and clone a legitimate key fob. The research resulted in three CVEs assigned in 2026 and impacts products deployed across multiple markets. Attendees will learn how assumptions about rolling-code security can fail in practice and how these failures can be exploited in the real world.

SpeakerBio: Danilo Erazo, Ekoparty, PCA Cybersecurity

Danilo Erazo is a Security Researcher at PCAutomotive in Budapest, Hungary. He has reported critical vulnerabilities to KIA Corporation, KIA Ecuador, Suzuki Motor Corporation, Calix Inc., Realtek Semiconductor Corp., and multiple Latin American banks. He is the organizer of the Car Hacking Village at Ekoparty, founder of the PWNORDIE security conference, and a speaker at Re/verse 2026, Secure Our Streets 2025, REcon 2025, Hardwear USA 2025, etc

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Contests - Sunday - 10:00-11:59 PDT

Title: Untechnical

Tags: Untechnical | Contest

When: Sunday, Aug 9, 10:00 - 11:59 PDT

Where: LVCCW Level 1 Hall 1 103 (Untechnical) - [Map](#)

Description:

In the age of AI hacking is reclaiming itself as more a mindset than strictly technical skill. If you're a DEFCON attendee that lack the technical skills to compete in traditional hacking challenges, but still love thinking outside the box: untechnical is for you.

Untechnical is a contest designed to rely 100% on lateral/abstract thinking without needing anything beyond an understanding of high school math.

Participant Prerequisites

Need to understand basic math and enjoy thinking outside the box. Oh, and you need an email address.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Contests - Friday - 10:00-17:59 PDT

Title: Untechnical

Tags: Untechnical | Contest

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 103 (Untechnical) - [Map](#)

Description:

In the age of AI hacking is reclaiming itself as more a mindset than strictly technical skill. If you're a DEFCON attendee that lack the technical skills to compete in traditional hacking challenges, but still love thinking outside the box: untechnical is for you.

Untechnical is a contest designed to rely 100% on lateral/abstract thinking without needing anything beyond an understanding of high school math.

Participant Prerequisites

Need to understand basic math and enjoy thinking outside the box. Oh, and you need an email address.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Contests - Saturday - 10:00-17:59 PDT

Title: Untechnical

Tags: Untechnical | Contest

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 103 (Untechnical) - [Map](#)

Description:

In the age of AI hacking is reclaiming itself as more a mindset than strictly technical skill. If you're a DEFCON attendee that lack the technical skills to compete in traditional hacking challenges, but still love thinking outside the box: untechnical is for you.

Untechnical is a contest designed to rely 100% on lateral/abstract thinking without needing anything beyond an understanding of high school math.

Participant Prerequisites

Need to understand basic math and enjoy thinking outside the box. Oh, and you need an email address.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Veilid- the Next Gen of privacy

Tags: DCNextGen | Creator Talk/Panel | Youth

When: Friday, Aug 7, 16:00 - 16:30 PDT

Where: LVCCW Level 3 W316 (DC NextGen) - [Map](#)

Description:

In this talk, medus4 will go over how the data economy insidiously invades everyone's privacy, and how Veilid is helping fight back against that. Will include a brief lesson on the history of privacy software, and how Veilid can assist everyone (including youth!) to make a better internet for all!

SpeakerBio: medus4

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Very Pwned: Hacking Verifone's card machine three times in a row

Tags: DEF CON Official Talk | Demo | Exploit

When: Saturday, Aug 8, 11:00 - 11:59 PDT

Where: LVCCW Level 1 Hall 3 903 (Main Track 5) - [Map](#)

Description:

Everyday billions of credit card transactions are made worldwide, with the vast majority being done on purpose-built card machines. In the USA alone, nearly 400 million transactions are performed per day on these popular devices present in nearly every retail store. In this talk, I'll focus on a widely deployed Verifone product line of card machines, with an estimated global deployment of over one million units. For several consecutive years I conducted an annual security assessment on these devices, until a pattern emerged: I'd arrive at the assessment, find a fresh set of vulnerabilities, gain root access, and then have Verifone patch the devices — only for me to return the following year and gain root access in a new way. I'll demonstrate the three separate attack chains I discovered, two of which only required network access to the target. I'll also detail additional vulnerabilities that could be used to disable hardening features such as grsecurity, including the ability to modify the file system to gain persistent access. Next, I'll show how an attacker could leverage this access to continuously capture credit card information - contrary to the device's security claims. Finally, in a homage to trixr4skids' DEF CON 25 talk in which he hacked an older series of Verifone's devices, I'll also run Doom.

DEF CON 25 - trixr4skids' DOOMed Point of Sale Systems CCC May Contain Hackers2022 - Thomas Rinsma's Payment terminals as general purpose (game-)computers

SpeakerBio: Reino Mostert, Orange Cyberdefense

Reino is a hacker who has been working as a penetration tester for the past decade. He has hacked various payment systems - from credit card devices all the way to payment switches, and has given talks at numerous cons. He enjoys coffee and hacking.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Social Gatherings/Events - Saturday - 21:00-00:59 PDT

Title: VETCON 2026 PARTY

Tags: Party | VETCON

When: Saturday, Aug 8, 21:00 - 00:59 PDT

Where: LVCCW Level 3 W326 (Vetcon) - [Map](#)

Description:

DEF CON is renowned for bringing together some of the brightest minds in technology and security. By participating in VETCON, you have the chance to highlight the critical role veterans play in this landscape and explore how technology can support and enhance their lives.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Vibe Check: Exploiting Developer Trust from Prompt Injections to Weaponized Repos

Tags: Malware Village | Creator Talk/Panel

When: Friday, Aug 7, 15:45 - 16:25 PDT

Where: LVCCW Level 1 Hall 2 600 (Malware Village) Talks - [Map](#)

Description:

"Do you trust the authors of the files in this folder?" It's a prompt modern IDEs throw at developers, and most click past it by reflex. But as vibe coding, AI-assisted tooling, and automated agents accelerate software development, that implicit trust in established tools like VS Code and authoritative sources like GitHub has become a critical, highly exploitable attack surface and malware delivery channel - especially for non-technical vibe coders.

This hands-on workshop places attendees directly in the mindset of an attacker targeting modern development environments. We move beyond traditional social engineering and focus on how trust is abused through the tools developers rely on every day: IDEs, agent harnesses, and package managers. After dissecting recent real-world cases of developer-targeted attacks and AI-agent vulnerabilities, we transition into labs where participants build and execute their own PoCs - including constructing malicious repositories from scratch to trigger invisible code execution on folder open, weaponizing hidden prompt injections to drive AI agents into running attacker-controlled commands, and standing up a custom "Claude Code"- style agent harness to attack ourselves.

Agenda: ðŸ“œHow your trusted IDEs betray you by executing malicious commands automatically ðŸ“œHow agent harnesses like Claude Code and Gemini CLI can be abused across multiple trust boundaries ðŸ“œHow package managers like npm turn seemingly harmless actions, like a routine package update, into full compromise

Bring a laptop - we'll get our hands dirty and hack ourselves together.

SpeakerBio: Michael Chan, Senior Offensive Security Consultant at KPMG Canada

Michael is a social scientist turned hacker. He started by studying human behaviour and trust at Oxford - now he brings that lens into offensive security, validating and breaking the assumptions built into applications, systems, and organizations. As a Senior Offensive Security Consultant at KPMG Canada, Michael works across application security, threat modelling, and adversary simulation. Outside of work, he spends most of his time learning, building, breaking fun new tech (yes AI included), and engaging with local cyber communities.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Vibe Coding Your Way to a Fully Functional Open-Source Intelligence Platform

Tags: Recon Village | Creator Workshop

When: Saturday, Aug 8, 15:20 - 17:50 PDT

Where: LVCCW Level 1 Hall 2 501 (Recon Village) - [Map](#)

Description:

Everyone is talking about vibe coding, but most examples stop at TODO apps, landing pages, or simple CRUD applications. This workshop goes far beyond that.

Participants will use modern AI coding agents to build a real-world Open-Source Intelligence (OSINT) platform from scratch designed to aggregate and visualize intelligence data on an interactive 3D globe.

Rather than simply watching a demo, attendees will actively build the application alongside the instructor while learning the mindset, prompting techniques, and engineering workflow required to successfully collaborate with AI coding assistants.

The workshop begins with the fundamentals of vibe coding: what it actually is, why it works, where it fails, and how to communicate effectively with AI agents. Participants will learn practical prompting strategies, iterative development techniques, and methods for breaking large software systems into manageable tasks that AI can successfully implement.

From there, we'll progressively build an intelligence dashboard capable of consuming and visualizing multiple real-time OSINT sources, including flight tracking, satellite positions, earthquake feeds, maritime traffic, and other publicly available intelligence signals. Along the way, participants will generate modern user interfaces, integrate external APIs, debug AI-generated code, and learn when to trust the model and when not to.

Rather than treating AI as a code generator, this workshop teaches attendees how to use AI as an engineering partner capable of dramatically increasing development velocity while still maintaining high-quality software.

By the end of the workshop, every participant will have:

1. A working open-source intelligence platform running locally
2. A practical workflow for building complex software using AI coding agents
3. A reusable prompting framework applicable to future projects
4. Experience integrating multiple public OSINT data sources
5. An understanding of the strengths and limitations of AI-assisted software development
6. A roadmap for continuing to extend the platform after the workshop

The workshop is based on the open-source project: <https://github.com/Alevsk/respondent-community>

Workshop Outline (150 Minutes)

Part 1 – Introduction to Vibe Coding (20 min)

- What vibe coding actually means
 - Mental models for collaborating with AI
 - Selecting the right AI model for the task
 - Understanding agentic coding workflows
 - Common mistakes and misconceptions
-

Part 2 – Prompt Engineering for Software Development (25 min)

- Structuring prompts that produce maintainable code
 - Breaking large systems into incremental tasks
 - Designing software through conversation
 - Iterating instead of regenerating
 - Knowing when to intervene manually
-

Part 3 – Building the Intelligence Platform (75 min)

Participants will build the platform together while learning how to:

- Generate a modern frontend
 - Create a real-time 3D globe visualization
 - Integrate multiple public OSINT APIs
 - Display flights, satellites, earthquakes, ships, and additional intelligence feeds
 - Build reusable UI components with AI
 - Debug AI-generated code
 - Refactor and improve generated implementations
 - Continue extending the application using AI as a development partner
-

Part 4 – Lessons Learned & Advanced Techniques (20 min)

- What AI does well
- Where AI still struggles
- Managing technical debt
- Building larger projects with AI
- Cost optimization strategies
- Recommended workflows and tooling
- Future directions for AI-assisted engineering

SpeakerBio: Lenin Alevski, Security Engineer at Google

Lenin Alevski is a Full Stack Engineer and generalist with a lot of passion for Information Security. Currently working as a Security Engineer at Google. Lenin specializes in building and maintaining Distributed Systems, Application Security and Cloud Security in general. Lenin loves to play CTFs, contributing to open-source and writing about security and privacy on his personal blog <https://www.alevsk.com>.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Payment Village - Saturday - 11:00-11:20 PDT

Title: Victim as a Service: Engaging with Trust-Based Scams Using AI

Tags: Payment Village | Creator Talk/Panel

When: Saturday, Aug 8, 11:00 - 11:20 PDT

Where: LVCCW Level 2 W204-205 (Payment Village) - [Map](#)

Description:

Pig butchering and other interactive online scams build trust over weeks to months, making them both highly effective and extremely difficult to study. In this talk, I will describe how we measure ground truth on this difficult and growing ecosystem.

First, I'll describe the design of an LLM-driven system that can sustain realistic, long-term engagement with scammers for weeks to months, enabling large-scale investigation of their tactics in the wild. I will discuss how we attract scam attempts, maintain thousands of convincing dialogues over time, and navigate the "milestones" scammers use to advance victims toward payment. I'll end with what this approach uncovered about scammer workflows (such as the "cross-platform" jump the majority of them use) and how this measurement drives understanding of the pig-butchering ecosystem to power data-driven scam defenses in the payments ecosystem.

SpeakerBio: Ariana Mirian, Security Researcher, BeeSafe AI

Security researcher focused on empirical measurement; currently drives data-driven methods to catch trust-based scams at BeeSafe AI, after leading measurement research at Censys. PhD in Computer Science and Engineering, UC San Diego.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Social Engineering Community Village - Friday - 08:45-08:59 PDT

Title: Village Greeting

Tags: Social Engineering Community Village | Creator Talk/Panel

When: Friday, Aug 7, 08:45 - 08:59 PDT

Where: LVCCW Level 3 W317-319 (Social Engineering Community Village) - [Map](#)

Description:

Join the founders for a preview of what' s happening in the Village this year.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Maker's Village - Sunday - 13:30-13:59 PDT

Title: Visable Mending, repair and reinforce

Tags: Maker's Village | Creator Event/Activity

When: Sunday, Aug 9, 13:30 - 13:59 PDT

Where: LVCCW Level 1 Hall 1 301 (Makers' Village) - [Map](#)

Description:

We'll be going over the types of tools, stitches. And techniques that go into mending, darning, and reinforcing clothes.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: VoiceLock: Offline, Robust On-Device Speech Transcription

Tags: Intro/Beginner | AI | DEF CON Demo Labs | Hardware/IoT | Mobile | Offense/Red Team | Threat Intel/Hunting | DEF CON Demo Labs

When: Saturday, Aug 8, 16:00 - 16:45 PDT

Where: LVCCW Level 1 Hall 3 1003 (Demo Labs Track 3) - [Map](#)

Description:

VoiceLock analyzes audio to identify speakers, count participants, and understand what each person said and discussed, just from a microphone. The self-contained, entirely offline system is designed for continuous, long-term use cases of 72 to 168 hours or more. The system runs entirely on-device, with high accuracy as tested on datasets and in the real world. Key innovations include an on-device vector database for fast speaker-similarity search and robust noise reduction, which greatly improve transcript accuracy. The output is a transcript with name labels. The system is fast enough to transcribe and report in under a minute. Code is written as an open-source Python module with a provided runtime and setup script to enable quick deployment on IoT devices. The system has been tested in challenging environments, including high noise levels, many speakers/arguments, and a lecture-style format. We present a live demo, technical details, and a short runtime tutorial.

Speakers:Ayaan Qayyum,Parag Kalay

SpeakerBio: Ayaan Qayyum

Ayaan is an MS in engineering student at Columbia University. His research interests include mobile computing, applied machine learning, edge AI, and data science. He is an expert in understanding customer needs and use cases to solve real-world problems.

SpeakerBio: Parag Kalay

Parag is a Biomedical Engineering MS student at Columbia University, combining expertise in CAD, rapid prototyping, and data-driven design to transform concepts into functional technologies under tight technical constraints. Skilled in translating clinical needs into robust engineering solutions from initial sketches to validated prototypes.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: VoiceLock: Offline, Robust On-Device Speech Transcription

Tags: Intro/Beginner | AI | DEF CON Demo Labs | Hardware/IoT | Mobile | Offense/Red Team | Threat Intel/Hunting | DEF CON Demo Labs

When: Friday, Aug 7, 12:00 - 12:45 PDT

Where: LVCCW Level 1 Hall 3 1003 (Demo Labs Track 3) - [Map](#)

Description:

VoiceLock analyzes audio to identify speakers, count participants, and understand what each person said and discussed, just from a microphone. The self-contained, entirely offline system is designed for continuous, long-term use cases of 72 to 168 hours or more. The system runs entirely on-device, with high accuracy as tested on datasets and in the real world. Key innovations include an on-device vector database for fast speaker-similarity search and robust noise reduction, which greatly improve transcript accuracy. The output is a transcript with name labels. The system is fast enough to transcribe and report in under a minute. Code is written as an open-source Python module with a provided runtime and setup script to enable quick deployment on IoT devices. The system has been tested in challenging environments, including high noise levels, many speakers/arguments, and a lecture-style format. We present a live demo, technical details, and a short runtime tutorial.

Speakers:Ayaan Qayyum,Parag Kalay

SpeakerBio: Ayaan Qayyum

Ayaan is an MS in engineering student at Columbia University. His research interests include mobile computing, applied machine learning, edge AI, and data science. He is an expert in understanding customer needs and use cases to solve real-world problems.

SpeakerBio: Parag Kalay

Parag is a Biomedical Engineering MS student at Columbia University, combining expertise in CAD, rapid prototyping, and data-driven design to transform concepts into functional technologies under tight technical constraints. Skilled in translating clinical needs into robust engineering solutions from initial sketches to validated prototypes.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Voting Village Keynote - The Paper Chase

Tags: Voting Village | Creator Talk/Panel

When: Friday, Aug 7, 12:00 - 12:45 PDT

Where: LVCCW Level 2 W220 (Voting Village) (Voting Village Talks) - [Map](#)

Description:

The 2000 presidential election was decided by Florida's "hanging chads"—flaws in the punchcard voting system used there at the time. In response, Congress passed the Help America Vote Act (HAVA), providing states with substantial funding (released in 2003) to replace punchcard systems with electronic voting machines (DREs), which were promoted as more secure, accurate, and accessible. As Majority Leader of the California State Assembly, Kevin Shelley authored the state's vote-by-mail program and other voting reforms. He was elected California Secretary of State in 2002 on a platform of expanding voter participation. Within his first month in office, however, David Dill brought him extensive documentation raising serious concerns about electronic voting security.

Shelley found the material compelling enough to form a touchscreen task force to study potential security issues and the need for a voter-verified paper audit trail. When the task force's findings, released months later, proved inconclusive, Shelley remained convinced further action was necessary. In November 2003, he launched an independent audit of California's voting systems and mandated that all touchscreen machines include a voter-verified paper audit trail—a move local election officials and voting rights advocates criticized as unnecessary and irresponsible, insisting the machines were already secure.

Ahead of the March 2004 election, Shelley imposed additional security requirements on touchscreen machines and required that paper ballots remain available; some counties defied the order. Later that year, he banned certain Diebold machines outright, decertified all touchscreen systems until security measures were met, asked the attorney general to pursue civil and criminal action against Diebold, and set up a parallel system to monitor the equipment's use.

Several lawsuits challenged these measures. Courts upheld Shelley's actions in every case. In her inaugural address as California Secretary of State in 2007, Deborah Bowen stated "Kevin Shelley had the hard work of evaluating new kinds of voting systems at a very, very early stage, and guess what – it turns out that he was right on a great many issues that had at their core the security and accuracy of the vote."

SpeakerBio: Kevin Shelley

Kevin Shelley is a former California Secretary of State and State Assembly leader recognized as a trailblazer in election integrity efforts. Mr. Shelley's political involvement began in 1978 as a staff member to U.S. Representatives Phil and Sala Burton. His own political career began in 1990, when he was elected to the San Francisco Board of Supervisors, serving twice as Board President. Elected to the California State Assembly in 1996, serving as Majority Leader, he championed the rights of workers, fought to protect the environment, and championed corporate accountability.

Mr. Shelley, was elected Secretary of State in 2002. As the state's Chief Election Officer, he is credited with improving voter participation, overseeing the historic Gubernatorial recall election on 2003, and decertifying problematic electronic voting machines. He established the first in the nation standards for accessible voter-verified paper audit trails to be used with direct recording electronic (DRE) voting machines in California.

After leaving State government in 2005, he became Special Counsel to Berman Tabacco, a law firm representing victims of corporate fraud. Currently he serves as Vice-Chair of Verified Voting, addressing issues of election security, and is focused on ensuring our upcoming November elections and beyond are safe and secure.

He is the son of Jack Shelley, a former San Francisco mayor, U.S. congressman and California state senator.



Voting Village - Sunday - 10:00-13:59 PDT

Title: Voting Village Lab

Tags: Voting Village | Creator Event/Activity

When: Sunday, Aug 9, 10:00 - 13:59 PDT

Where: LVCCW Level 2 W219 (Voting Village) (Voting Village Lab) - [Map](#)

Description:

The Voting Village Lab is a hands-on, self-directed workshop space where attendees can learn about and experiment with dozens of different pieces of election equipment used in current and past US elections.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Voting Village - Saturday - 10:00-17:59 PDT

Title: Voting Village Lab

Tags: Voting Village | Creator Event/Activity

When: Saturday, Aug 8, 10:00 - 17:59 PDT

Where: LVCCW Level 2 W219 (Voting Village) (Voting Village Lab) - [Map](#)

Description:

The Voting Village Lab is a hands-on, self-directed workshop space where attendees can learn about and experiment with dozens of different pieces of election equipment used in current and past US elections.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Voting Village - Friday - 10:00-17:59 PDT

Title: Voting Village Lab

Tags: Voting Village | Creator Event/Activity

When: Friday, Aug 7, 10:00 - 17:59 PDT

Where: LVCCW Level 2 W219 (Voting Village) (Voting Village Lab) - [Map](#)

Description:

The Voting Village Lab is a hands-on, self-directed workshop space where attendees can learn about and experiment with dozens of different pieces of election equipment used in current and past US elections.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

The Diana Initiative - Saturday - 13:10-13:20 PDT

Title: Voting Village Tour

Tags: The Diana Initiative | Creator Tour

When: Saturday, Aug 8, 13:10 - 13:20 PDT

Where: LVCCW Level 1 South Lobby / Atrium - [Map](#)

Description:

Interested in visiting Voting Village but afraid to go by yourself? The Diana Initiative is hosting tours! Follow a volunteer to Voting Village and be introduced to the community and activities inside!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

DEF CON Training - Tuesday - 08:30-17:30 PDT

Title: VS: S-RAD (Satellite-Radio Analysis & Disruption)

Tags: DEF CON Training (Paid) (2-day) | DEF CON Training

When: Tuesday, Aug 11, 08:30 - 17:30 PDT

Where: LVCCW Level 2 W201 (HDA Community) - [Map](#)

Description:

Speakers: Andrzej Olchawa, Ricardo Fradique, André Cirne

SpeakerBio: Andrzej Olchawa

No BIO available

SpeakerBio: Ricardo Fradique

No BIO available

SpeakerBio: André Cirne

No BIO available

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

DEF CON Training - Monday - 08:30-17:30 PDT

Title: VS: S-RAD (Satellite-Radio Analysis & Disruption)

Tags: DEF CON Training (Paid) (2-day) | DEF CON Training

When: Monday, Aug 10, 08:30 - 17:30 PDT

Where: LVCCW Level 2 W201 (HDA Community) - [Map](#)

Description:

Speakers: Andrzej Olchawa, Ricardo Fradique, André Cirne

SpeakerBio: Andrzej Olchawa

No BIO available

SpeakerBio: Ricardo Fradique

No BIO available

SpeakerBio: André Cirne

No BIO available



[Return to Index](#) - Add to Google

- ics [Calendar](#) file

Payment Village - Sunday - 10:30-10:50 PDT

Title: Wall of Wallets Workshop (Intro to Wall of Wallets Challenge)

Tags: Payment Village | Creator Workshop

When: Sunday, Aug 9, 10:30 - 10:50 PDT

Where: LVCCW Level 2 W204-205 (Payment Village) - [Map](#)

Description:

Wall of Wallets is a hands-on CTF challenge where the goal is simple: collect as many mock payment card details as you can from other participants. Using intentionally vulnerable services in a safe, isolated environment, you'll learn how common implementation mistakes expose sensitive data. Compete to top the Wall of Wallets leaderboard while discovering the real-world techniques attackers use and, importantly, how to defend against them.

SpeakerBio: Dan Borgogno, Security Researcher at Faraday

Dan Borgogno is a security researcher, backend developer, security engineer and international speaker with years of experience on mobile, hardware, IoT and web application hacking.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Payment Village - Friday - 13:00-13:20 PDT

Title: Wall of Wallets Workshop (Intro to Wall of Wallets Challenge)

Tags: Payment Village | Creator Workshop

When: Friday, Aug 7, 13:00 - 13:20 PDT

Where: LVCCW Level 2 W204-205 (Payment Village) - [Map](#)

Description:

Wall of Wallets is a hands-on CTF challenge where the goal is simple: collect as many mock payment card details as you can from other participants. Using intentionally vulnerable services in a safe, isolated environment, you'll learn how common implementation mistakes expose sensitive data. Compete to top the Wall of Wallets leaderboard while discovering the real-world techniques attackers use and, importantly, how to defend against them.

SpeakerBio: Dan Borgogno, Security Researcher at Faraday

Dan Borgogno is a security researcher, backend developer, security engineer and international speaker with years of experience on mobile, hardware, IoT and web application hacking.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Wand Protocol: Full-Chain Attack on an FDA-Listed Fertility Analyzer

Tags: Biohacking Village | Creator Talk/Panel

When: Sunday, Aug 9, 10:30 - 10:59 PDT

Where: LVCCW Level 1 Hall 3 1104 (Creator Stage 4) - [Map](#)

Description:

This year's BHV theme is access. This talk is about what happens when access is granted to everyone who should not have it, and about what happens to patient data once it leaves the device. We conducted a full security assessment of a shipping consumer fertility hormone analyzer — an FDA-listed device used by millions of people to track LH, FSH, estrogen, and progesterone. In a post-Dobbs environment, those measurements are not just health data. In 14 states, they are potential legal evidence. We found no authentication anywhere in the stack. From BLE proximity, any attacker within approximately 30 meters can silently rebind the device to an attacker-controlled account in under 15 seconds using a ~\$10 dongle and open-source tools. No credentials. No pairing prompt. No notification to the user. The protocol works exactly as designed. The companion app identifies hardware by a substring check on the BLE advertisement name. Any peripheral advertising a matching name receives the user's live API session token during the app's own handshake. That token grants access to the complete hormone history, miscarriage status, PCOS diagnosis, and fertility treatment records of any user whose phone comes within range. The cloud login endpoint issues session tokens without verifying the password. Email address alone grants full account access. A hardcoded API key in the distributed APK grants read and write access to approximately 659,000 user health profiles with no per-object authorization. Reproductive health data — including miscarriage history — transmits to analytics vendors, an advertising pixel, and a customer data platform headquartered in Russia on every session open. This talk presents the full attack chain with live demos, maps each finding to FDA's February 2026 premarket cybersecurity guidance, and closes with three concrete implementation decisions that would have prevented all of it. Coordinated disclosure submitted to vendor, FDA CDRH, and CISA. All testing on researcher-owned hardware and accounts.

SpeakerBio: Gigi Xiaoqing Liu

Gigi Liu is a graduate security researcher at Northeastern's Security And Privacy Research (SPQR) Group under Professor Kevin Fu, where her work covers embedded systems security, medical device attack surfaces, and AI-generated media detection. She interns at Lila Sciences as a Security and Cloud Engineer, building enterprise-wide agentic AI security infrastructure and detection capabilities for unauthorized AI activity across cloud and SaaS environments.

Her technical work spans wireless protocol reverse engineering, binary exploitation, web and mobile reverse engineering, cloud and AI security. She has applied these skills across medical hardware, automotive platforms, and enterprise cloud environments — from BLE command injection on FDA-listed devices to CarPlay API exploitation to building agentic AI detection controls at scale. As a UCLA psychobiology alum with a consulting background, she brings a multidisciplinary lens to every system: understand what it's designed to do first, then find where it breaks.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Noob Community - Saturday - 10:00-10:15 PDT

Title: Wanna Hack Space ? Why? Is it out of this world?

Tags: Noob Community | Creator Talk/Panel

When: Saturday, Aug 8, 10:00 - 10:15 PDT

Where: LVCCW Level 1 Hall 4 1417 (Noob Community) - [Map](#)

Description:

What can you do to become involved? How to get into the Space Satellites & Cybersecurity? There is some crossover of cybersecurity skills with Space and Satellites. Did you know Linux is increasingly used in space for high-reliability, low-cost applications, with specialized, hardened distributions now addressing radiation, security, and real-time demands. Review SPARTA:MITRE for Space! NASA Open Source Software FPrime(F'), AMSAT CUBESAT SIM.
<https://ct3sathack.cacyber.net/>

SpeakerBio: Henry Danielson Hankashyyyk

No BIO available

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Radio Frequency Village - Sunday - 10:00-11:55 PDT

Title: WarDriver Meetup

Tags: Radio Frequency Village | Creator Event/Activity

When: Sunday, Aug 9, 10:00 - 11:55 PDT

Where: LVCCW Level 1 Hall 1 409 (Radio Frequency Village) - [Map](#)

Description:



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: WASM Was Not the Boundary: Sandcastles, Not Sandboxes

Tags: DEF CON Official Talk | Demo | Exploit

When: Friday, Aug 7, 14:30 - 15:30 PDT

Where: LVCCW Level 1 Hall 3 1007 (Main Track 2) - [Map](#)

Description:

Pyodide is often treated as a ready-made sandbox: block os, block js, and untrusted Python is assumed to stay inside WebAssembly. In n8n and the other products we tested, that assumption failed. When ctypes or reflection remained reachable, attacker-controlled Python could cross from CPython-in-WASM into the Emscripten/JavaScript host boundary the product actually relied on.

We show this as an architectural failure, not a one-off bug. In Node.js embeddings, that boundary break typically becomes immediate host-side code execution because the escaped code lands in a runtime with no native permission model. In Deno embeddings, the same break still reaches the embedding runtime, but the final blast radius depends on the permissions the product granted; in one default configuration, that still meant full RCE. In CI environments, the same mistake turns tests and build steps into a supply-chain risk because the escaped code runs next to tokens, secrets, and release artifacts.

Across workflow automation, spreadsheets, AI agents, desktop wrappers, and build tooling, we found seven escapes, two public CVEs, and multiple additional disclosures. Attendees leave with a precise mental model of where Pyodide isolation actually ends, how to test similar deployments, and how to harden them beyond fragile denylists.

- Pyodide documentation. Pyodide is CPython compiled with Emscripten to WebAssembly and embedded in a JavaScript host; this host-embedding model is central to our analysis. <https://pyodide.org/>
 - ◆ Emscripten API documentation for `emscripten_run_script*`. These APIs are the JavaScript-execution bridge we reached from Pyodide via ctypes. <https://emscripten.org/>
 - ◆ Lehmann et al., "Everything Old is New Again: Binary Security of WebAssembly," USENIX Security 2020.
 - ◆ Bosamiya et al., "Provably-Safe Multilingual Software Sandboxing using WebAssembly," USENIX Security 2022.
 - ◆ Zhao et al., "Remote Code Execution from SSTI in the Sandbox: Cracking the Sandbox of Template Engines via Isolation-Aware Attack," USENIX Security 2023.
 - ◆ Public advisories for two instances from this research: CVE-2025-68668 / GHSA-62r4-hw23-cc8v (n8n) CVE-2026-24002 / GHSA-7xvx-8pf2-pv5g (Grist)

Speakers: Saar Pearl, Vladimir "G1ND1L4" Tokarev

SpeakerBio: Saar Pearl, Cyera

Saar Pearl is a security researcher at Cyera. He specializes in offensive security and vulnerability research across cloud infrastructure and SaaS platforms, focusing on identity and access controls, architectural weaknesses and exploit development.

SpeakerBio: Vladimir "G1ND1L4" Tokarev, Cyera

Vladimir Tokarev is a vulnerability researcher tech lead at Cyera, specializing in Cloud, IoT/OT, Windows, Linux, and AI vulnerability research and exploit. Talks: Black Hat USA 2024 and 2023, DEF CON 33 Recon Village 2025, CodeBlue 2025, RSA 2024.



Title: Watching Norway's Election

Tags: Voting Village | Creator Talk/Panel

When: Friday, Aug 7, 16:30 - 16:59 PDT

Where: LVCCW Level 2 W220 (Voting Village) (Voting Village Talks) - [Map](#)

Description:

What can an ordinary citizen — equipped with curiosity, a camera, and a little code — actually learn about how their elections are run? In 2025 the speaker set out to find out, observing Norway's national election from both the inside and the outside. The results ranged from the illuminating to the absurd: scraping official result protocols into structured JSON for independent analysis; working two prior elections "undercover" as a paid poll worker; spotting an unsealed ballot box where the chain of custody should have been airtight; and, on count night, being removed from a municipal counting center by police.

This talk turns those experiences into a practical, cross-border playbook for independent election observation. Norway runs paper ballots, manual counts, and publishes machine-readable results — yet transparency still has gaps, and getting access can be surprisingly adversarial. Using Norway as a concrete case study, the speaker shows how anyone — hacker, researcher, or concerned voter — can document a count, capture and analyze published election data, spot anomalies, and do it all legally and credibly.

Attendees leave with concrete methods: what to watch for, how to record it, how to turn official data dumps into analyzable datasets, and how to handle officials when curiosity is mistaken for a threat. The core message is empowerment: election integrity is not a spectator sport reserved for institutions. The more eyes — and code — on the process, the stronger democracies become, in the U.S. and everywhere else.

SpeakerBio: Hallvard Nygard

Hallvard Nygård is an independent security researcher and election observer based in Norway. He has spent recent years turning a developer's toolkit on the machinery of democracy: scraping and analyzing published election data, observing counts in person, and working as a paid poll worker (valgmedarbeider) during Norway's 2021 and 2023 elections to understand the process from the inside.

His independent observation of Norway's 2025 election drew media attention after he was removed from municipal counting center by police — an episode he now uses to illustrate both the promise and the friction of citizen oversight.

Hallvard is a frequent speaker on the Norwegian conference and security-community circuit, including Sikkerhetsfestivalen, JavaZone, NDC Oslo, TDC, and HelloStavanger, as well as meetups such as OWASP Oslo, Stavanger Security Hangout (SSH), and an Oslo election meetup. He is a vocal advocate for hands-on, hacker-style scrutiny of elections and for empowering ordinary citizens to observe and document their own local democratic processes. Online he can be found at hallny.bsky.social and as [@hallny](#) on X.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: We Pwn Your Phone, We Pwn Your Vote (Demo and Panel)

Tags: Demo | Voting Village | Creator Talk/Panel

When: Friday, Aug 7, 17:00 - 17:45 PDT

Where: LVCCW Level 2 W220 (Voting Village) (Voting Village Talks) - [Map](#)

Description:

Mobile voting proposals increasingly rest on a single assertion: that modern smartphones, with their secure enclaves, sandboxed apps, and encrypted communications, provide a sufficiently trusted platform for remote ballot casting. This talk demonstrates, live and on stage, why that assertion is false.

Using a weaponized n-day exploit chain (CVE-2025-43529) against a now patched but-still-widely-deployed iOS version, we will compromise a live iPhone in front of the audience. The phone's screen will display nothing but a Wikipedia article. The user will have no indication that anything has happened. Meanwhile, a second screen will show the audience exactly what is being taken from the device in real time: text messages, messaging app databases (Signal, WhatsApp, Telegram), photos, saved passwords, WiFi credentials, location history, and contacts, all exfiltrated with zero on-device artifacts.

The exploit achieves full kernel read/write and root filesystem access. At that level of compromise, no app on the device can be trusted: not voting apps, not authenticators, not encrypted messengers. The encryption keys, cloud session tokens, and biometric material that apps rely on to prove "this is the legitimate voter" are all accessible to an attacker with this level of access.

This specific vulnerability is patched. But two facts remain: (1) the targeted iOS version is still running on millions of devices worldwide, and (2) nation-state actors and sophisticated criminal organizations maintain working exploit chains against the latest iOS and Android versions, chains that have not been patched because they have not been discovered or disclosed. The tool we demonstrate is an n-day. The tools in active deployment against current devices are zero-days.

Speakers: Brian DeMuth, Matt Blaze, David Jefferson, Michael Specter

SpeakerBio: Brian DeMuth

Brian DeMuth, a "former" hacker, is an entrepreneur and investor who has spent his 28-year career supporting the U.S. National Security Mission, cybersecurity businesses, and nonprofits. Brian is co-founder and General Partner of the Riphean Investments National Security Fund, a venture-studio-style investment fund focused on technology investments that strengthen national security for the U.S. and its citizens. He is the Founder of Immortal Cyber, Inc., an advanced cybersecurity research and engineering firm providing offensive cyber delivery services and "Cyber-as-a-Service" for unique clients, and Co-Founder & CEO of RapidAscent, Inc., a scalable, task-based cyber apprenticeship solution addressing the historic shortage of technical personnel in the U.S. and worldwide. Brian also co-founded and chairs the board of the Cyber Bytes Foundation, a 501(c)(3) dedicated to building a unique cyber ecosystem of educational and outreach programs for the cyber workforce. A longtime advocate for election security, Brian serves on the Board of Directors of the Election Integrity Foundation, the 501(c)(3) behind the DEF CON Voting Village.

SpeakerBio: Matt Blaze

Matt Blaze is the McDevitt chair in Computer Science and Law at Georgetown University, where he studies problems at the intersection of technology and public policy. Election systems and voting technology are central focuses of his research. He led teams as part of the California TTBR and Ohio EVEREST studies that each found deep and fundamental weaknesses in different election technologies used by those states and the rest of the US. He has testified on technical risks in elections before the US Congress and other bodies numerous times. Blaze is a co-founder of the Voting Village and president of the Election Integrity Foundation.

SpeakerBio: David Jefferson

David Jefferson is an internationally recognized expert on voting systems and election technology, and an advisor to five successive California Secretaries of State. In 2004 he was coauthor of the SERVE Security Report detailing the security vulnerabilities in the Defense Department's proposed Internet voting system, leading to the cancellation of the program. In 2003 he was a member of the California Task Force on Touchscreen Voting, whose recommendations led to voter-verified paper audit trails for electronic voting machines. He has led half a dozen technical studies on reliability and security of voting systems, including the California Post-Election Audit Standards Working Group that produced the first government study of post-election auditing. He has served on the boards of directors of both the California Voter Foundation and Verified Voting, and is currently on the board of the Election Integrity Foundation that puts on the annual DEF CON Voting Village.

Dr. Jefferson received a BS in mathematics from Yale University, and a Ph.D. in computer science from Carnegie-Mellon University. From 1980 to 1994 he was a professor at the University of Southern California (USC) and then at UCLA. He is now retired from Lawrence Livermore National Laboratory where he conducted research in supercomputing and cyber security.

SpeakerBio: Michael Specter

Michael A. Specter is an Assistant Professor in Computer Science at Georgia Tech where he leads the SPDR Lab. Specter's interests are broadly on problems in systems security and applied cryptography, specifically on issues relevant to public policy. He joined Google after completing his PhD in Electrical Engineering and Computer Science at MIT, and previously served as research staff at MIT's Lincoln Laboratory. His research has been featured in congressional testimony, amicus briefs to the Supreme Court, and (repeatedly) in the popular press. He holds the 2023 Research Award from the Elections Verification Network and a Pioneer Award from the Electronic Frontier Foundation (EFF).



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Weaponization of Cellular Based IoT Technology – Leveraging Smart Devices to Gain a Foothold

Tags: IoT Village | Creator Talk/Panel

When: Saturday, Aug 8, 16:30 - 17:30 PDT

Where: LVCCW Level 1 Hall 3 1105 (Creator Stage 3) - [Map](#)

Description:

As IoT devices continue to integrate cellular technologies for communication, the potential risk for adversaries to weaponize the hardware's trust relationship and gain access to critical backend infrastructure grows exponentially. During this talk, we will present our research focused on how built-in cellular technology in IoT devices can be leveraged to gain access to and execute attacks against cloud services and backend private network environments. We will cover methods to modify IoT devices to take control over the installed cellular modules, allowing for injecting communications and establishing Man-in-the-Middle (MitM) traffic between the Micro Controller Units (MCU) and the cellular modules. We will demonstrate how control of onboard cellular communications could be used to launch attacks against the backend cloud infrastructure and network systems outside of the IoT device's intended purpose. During this presentation, we will demo and release proof-of-concept code to control the onboard cellular modules to accomplish these goals. We will also provide actionable defense strategies, including discussions around hardware design recommendations, interface access control settings, and methods for applying targeted mitigation techniques and processes so organizations can strengthen IoT trust boundaries and protect against this evolving class of cellular-based threats.

Speakers: Carlota Bindner, Deral Heiland

SpeakerBio: Carlota Bindner

No BIO available

SpeakerBio: Deral Heiland, Rapid7

Deral Heiland CISSP, serves as a Principal Security Researcher (IoT) for Rapid7. Deral has over 25 years of experience in the Information Technology field, and over the last 15+ years Deral's career has focused on security research, security assessments, penetration testing, and consulting for corporations and government agencies. Deral also has conducted security research on numerous technical subjects, releasing white papers, security advisories, and has presented the information at numerous national and international security conferences including Blackhat, Defcon, Shmoocon, DerbyCon, RSAC, Hack in Paris. Deral has been interviewed and quoted by several media outlets and publications including ABC World News Tonight, BBC, Consumer Reports, MIT Technical Review, SC Magazine, and The Register.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Weaponizing CloudFormation: Privilege Escalation via Infrastructure as Code in AWS

Tags: Cloud Village | Creator Event/Activity | Attack

When: Friday, Aug 7, 11:00 - 12:59 PDT

Where: LVCCW Level 3 W311 (Cloud Village Labs) A - [Map](#)

Description:

CloudFormation is widely trusted as a secure and declarative Infrastructure as Code (IaC) service inside AWS environments. In practice, however, CloudFormation frequently operates with permissions far beyond those of individual users, CI/CD pipelines, or developers. This workshop explores how attackers can abuse that trust model to achieve privilege escalation and persistence in realistic AWS environments.

In this fully hands-on offensive cloud security workshop, attendees will begin with limited IAM permissions and learn how to identify and exploit misconfigured CloudFormation execution roles using iam:PassRole, service roles, and Lambda-backed Custom Resources. Participants will weaponize CloudFormation templates to create persistence mechanisms inside service-scoped IAM paths without requiring direct administrative permissions.

The workshop emphasizes realistic cloud attack paths, delegated execution abuse, and the security risks introduced by over-permissioned automation. Attendees will also explore rollback abuse scenarios and learn how these attacks appear in CloudTrail and IAM logs.

SpeakerBio: Samanta Aranda

Samanta Aranda serves as a Managing Senior Consultant at Bishop Fox, leading security assessments and initiatives focused on strengthening organizations' technological resilience. She holds a degree in Electronics and Communications Engineering and a Master's in Computer Science and Technology Management. From the very beginning of her career, she found in cybersecurity not just a profession but a genuine passion. Over the years, she has collaborated with national and international firms such as KPMG, Scitum, EC-Council LATAM, and INFOTEC, contributing to projects that bridge technology, strategy, and security.

Samanta holds 16 professional certifications, including GPEN, GWAPT, CEH, and CND, and has been recognized as an EC-Council Certified Instructor, earning a place in the organization's Circle of Excellence in 2021. She blends technical expertise with a human and collaborative approach to security, firmly believing that shared knowledge is the strongest defense.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Weaponizing eBPF and XDP with Covert Triggered Reverse Shells

Tags: DEF CON Demo Labs | Intermediate | Defense/Blue Team | Malware | Offense/Red Team | Purple Team | DEF CON Demo Labs

When: Saturday, Aug 8, 16:00 - 16:45 PDT

Where: LVCCW Level 1 Hall 3 901 (Demo Labs Track 5) - [Map](#)

Description:

eBPF and XDP now underpin critical Linux infrastructure yet their kernel-level access creates a blind spot: adversaries can weaponize these primitives for stealth persistence that evades standard forensic tools. Current defenses are not equipped for this emerging threat.

We built Phantasma, an open-source eBPF implant, to expose this gap. It combines three kernel-level techniques: (1) XDP covert triggering that intercepts packets at the NIC driver before they reach the networking stack, firewalls, or packet capture systems (2) getdents64 syscall interception to hide processes from /proc, defeating ps, top, and all enumeration tools; and (3) bpf() syscall interception to cloak loaded eBPF objects from bpftool and forensic inspection.

We live-demonstrate the full attack chain deployment, self-cloaking, magic packet activation, and encrypted reverse shell showing the implant defeating packet capture, process listing, and BPF introspection simultaneously.

We then present the defenses this threat demands: kernel audit rules for bpf() syscalls, /sys/fs/bpf inspection, XDP attachment monitoring, and behavioral indicators. Attendees leave with detection rules, hardening steps, and a clear understanding of why eBPF must be treated as an attack surface, not just a defense tool.

SpeakerBio: Yll "0xBabar0ka" Berisha

I am an offensive security researcher with 2 years of experience in penetration testing, red teaming, and custom tooling. I am the creator of Phantasma, an open-source eBPF/XDP implant framework for stealth persistence research.

Professionally, I have worked at Sentry, conducting web, mobile, and internal/external network penetration tests. At Finbug, I contributed to a US Embassy-supported project assessing the cybersecurity posture of NGOs and media organizations in Kosovo, identifying issues such as XSS, directory listing, and IDOR vulnerabilities. At Starlabs, I built dark web monitoring tools using HaveIBeenPwned and LeakX APIs for automated credential leak detection.

I hold BSCP (Burp Suite Certified), CRT-ID (Certified Red Team Infra Dev), MCRTA (Multi Cloud Red Teamer), CISCO ETHICAL HACKER, and HACKWISER CAPT certifications. I placed 1st at the Iowa State Cyber Defense Competition and represented Kosovo at the 2024 ENISA European Cybersecurity Challenge in Turin.

I have presented at CyberZero on prompt injection attacks and deepfake-based social engineering at the TechRisk conference, and co-organized national and international CTFs designing real-world attack chain challenges.

I am also a member of DefCon Group Prishtina (DC38338), where I contribute to co-organizing meetups and community events.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Weaponizing eBPF and XDP with Covert Triggered Reverse Shells

Tags: DEF CON Demo Labs | Intermediate | Defense/Blue Team | Malware | Offense/Red Team | Purple Team | DEF CON Demo Labs

When: Friday, Aug 7, 12:00 - 12:45 PDT

Where: LVCCW Level 1 Hall 3 901 (Demo Labs Track 5) - [Map](#)

Description:

eBPF and XDP now underpin critical Linux infrastructure yet their kernel-level access creates a blind spot: adversaries can weaponize these primitives for stealth persistence that evades standard forensic tools. Current defenses are not equipped for this emerging threat.

We built Phantasma, an open-source eBPF implant, to expose this gap. It combines three kernel-level techniques: (1) XDP covert triggering that intercepts packets at the NIC driver before they reach the networking stack, firewalls, or packet capture systems (2) getdents64 syscall interception to hide processes from /proc, defeating ps, top, and all enumeration tools; and (3) bpf() syscall interception to cloak loaded eBPF objects from bpftool and forensic inspection.

We live-demonstrate the full attack chain deployment, self-cloaking, magic packet activation, and encrypted reverse shell showing the implant defeating packet capture, process listing, and BPF introspection simultaneously.

We then present the defenses this threat demands: kernel audit rules for bpf() syscalls, /sys/fs/bpf inspection, XDP attachment monitoring, and behavioral indicators. Attendees leave with detection rules, hardening steps, and a clear understanding of why eBPF must be treated as an attack surface, not just a defense tool.

SpeakerBio: Yll "0xBabar0ka" Berisha

I am an offensive security researcher with 2 years of experience in penetration testing, red teaming, and custom tooling. I am the creator of Phantasma, an open-source eBPF/XDP implant framework for stealth persistence research.

Professionally, I have worked at Sentry, conducting web, mobile, and internal/external network penetration tests. At Finbug, I contributed to a US Embassy-supported project assessing the cybersecurity posture of NGOs and media organizations in Kosovo, identifying issues such as XSS, directory listing, and IDOR vulnerabilities. At Starlabs, I built dark web monitoring tools using HaveIBeenPwned and LeakX APIs for automated credential leak detection.

I hold BSCP (Burp Suite Certified), CRT-ID (Certified Red Team Infra Dev), MCRTA (Multi Cloud Red Teamer), CISCO ETHICAL HACKER, and HACKWISER CAPT certifications. I placed 1st at the Iowa State Cyber Defense Competition and represented Kosovo at the 2024 ENISA European Cybersecurity Challenge in Turin.

I have presented at CyberZero on prompt injection attacks and deepfake-based social engineering at the TechRisk conference, and co-organized national and international CTFs designing real-world attack chain challenges.

I am also a member of DefCon Group Prishtina (DC38338), where I contribute to co-organizing meetups and community events.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Weaponizing Uselessness: Breaking SMM with the Slowest Instruction Ever Written

Tags: DEF CON Official Talk | Demo | Tool | Exploit

When: Friday, Aug 7, 10:00 - 10:30 PDT

Where: LVCCW Level 1 Hall 3 904 (Main Track 4) - [Map](#)

Description:

This is a talk about making your CPU go slow. Really, really, really slow.

It is also, somehow, a talk about breaking platform security on nearly every x86 system ever shipped, activating a hundred dormant CVEs, repeatedly ignoring processor specifications, racing intra-core interrupts, and finding a vulnerability that cannot be fixed.

But mostly, it's about going slow.

[Memory Sinkhole](#) [AMD Sinkclose](#) [Sandsifter](#) [EDK2](#)

SpeakerBio: Christopher "xoreaxeaxeax" Domas

Christopher Domas (@xoreaxeaxeax) is a security researcher primarily focused on firmware, hardware, and low level processor exploitation. He is best known for releasing impractical solutions to non-existent problems, including the world's first single instruction C compiler (M/o/Vfuscator), toolchains for generating images in program control flow graphs (REpsych), and Turing-machines in the vi text editor. His more relevant work includes the sandsifter processor fuzzer, rosenbridge backdoor, the binary visualization tool ..cantor.dust., and the memory sinkhole privilege escalation exploit.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Red Team Village - Friday - 12:00-13:59 PDT

Title: Web Hacking Bootcamp

Tags: Red Team Village | Misc

When: Friday, Aug 7, 12:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 1 309 (Red Team Village) Tactic Table 3 - [Map](#)

Description:

A beginner to intermediate hands-on web hacking bootcamp originally created for internal up-skilling. Hands on with both specific to module PortSwigger labs and a self-hosted Juice Shop instance running on Docker Desktop.

Presentation Outline: - Web Technology Foundations (Pre-requisite's on web-specific languages, encoding, HTTP request structure, some 'Hacker Mindset') - Web Hacking Foundations (What is an application proxy/setting up Burp Suite, 'auth' & 'auth', sessions & tokens, CORS, vocabvocab) - Web Hacking Modules (file upload attacks, SQL injection, JWT attacks, XSS, CSRF, XXE & business logic vulnerabilities)

After each major section, and in-between some of the hacking modules, we return to a self-hosted OWASP Juice Shop instance to try out new techniques learned. Each hacking module will end with related PortSwigger Web Security Academy labs which attendees will work through on their own with instructor support. (think: I walk around and give nudges as needed.)

All material being self-or-Portswigger hosted means that even if the time slot doesn't include sufficient lab time, attendees will be able to take what they heard and work on labs laid out or practice with Juice Shop on their own time. The main objective is to give attendees a minimum understanding of web tech & attacks that they feel empowered to dive in deeper from that point.

SpeakerBio: Emma Latuszek

Emma 'vhulf' Latuszek is an application developer turned breaker, who started her hacking career nearly a decade ago. She is an OSWE holder, Cyphercon safe-cracker and a verified cyborg (barely... but thanks DangerousThings!). Vhulf is esoteric and unusual, with a deep passion for music, hacking and high-energy instruction.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Web3 Security: Hacks, Scams, and Exploits

Tags: Cryptocurrency Village | Creator Talk/Panel

When: Saturday, Aug 8, 10:00 - 10:59 PDT

Where: LVCCW Level 1 Hall 3 1103 (Creator Stage 5) - [Map](#)

Description:

Why do Web3 users keep getting hacked even when the smart contracts are audited? This workshop examines the Web3 attack surface through three lenses: the client, the dApp frontend, and the blockchain, using real-world hacks, scams, and exploits to demonstrate how each layer can fail. Participants will conduct a live review of their own wallet approvals using revoke.cash and learn practical techniques for reducing risk. The workshop concludes with a forensic deep dive into the \$1.5 billion Bybit hack, where attendees will analyze the malicious transaction, compromised frontend, and on-chain evidence that enabled the largest cryptocurrency theft in history.

Speakers: Philip "AlephNull" Werlau, Kennashka DeSilva

SpeakerBio: Philip "AlephNull" Werlau, Founder, Flowstate Cyber

Philip is a cryptocurrency investigator and smart contract analyst specializing in DeFi, on-chain forensics, and blockchain security. Experienced in support of government agencies and private-sector clients in cryptocurrency fraud investigations, exploit analysis, fund tracing, and smart contract risk analysis, Philip's extensive familiarity with EVM ecosystems, blockchain analytics, and custom investigative tooling contributes to his work in government and industry.

SpeakerBio: Kennashka DeSilva

Kennashka DeSilva is a seasoned cybersecurity researcher with a strong track record of advancing security best practices in decentralized systems. She was a featured speaker at DEF CON 30's "Hacking & Defending Blockchain Applications" session, where she helped bridge the gap between traditional application security frameworks—such as the OWASP Top Ten—and the unique risks found in DEFI and smart contract ecosystems. Kennashka is also an active participant in the cybersecurity community, having contributed to multiple HackMiami events and served on the executive councils of Women in Cybersecurity Florida and Black Girls in Cyber, helping to advance diversity, mentorship, and professional development in the field. Her expertise spans vulnerability management, threat modeling, and policy-driven security in Web3 and enterprise systems.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Social Gatherings/Events - Thursday - 18:30-23:30 PDT

Title: Welcome Party at The Industrial

Tags: Party

When: Thursday, Aug 6, 18:30 - 23:30 PDT

Where: The Industrial

Description:

Kick off DEF CON at our official Welcome Party! We'll meet at [The Industrial](#) at 18:30.

Standby for details about shuttles from LVCC to The Industrial.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

DEF CON Talks - Friday - 10:00-10:30 PDT

Title: Welcome to DEF CON 34!

Tags: DEF CON Official Talk | DEF CON Communications

When: Friday, Aug 7, 10:00 - 10:30 PDT

Where: LVCCW Level 1 Hall 3 1006 (Main Track 1) - [Map](#)

Description:

SpeakerBio: Jeff "The Dark Tangent" Moss

Mr. Moss is an internet security expert and is the founder of both the Black Hat Briefings and DEF CON Hacking conferences.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

OSINT For Good Community - Friday - 11:45-12:15 PDT

Title: Welcome to OSINT4Good and Trace Labs

Tags: OSINT For Good Community | Creator Talk/Panel

When: Friday, Aug 7, 11:45 - 12:15 PDT

Where: LVCCW Level 1 Hall 4 1307 (OSINT4Good Community) Stage - [Map](#)

Description:

This overview session will talk about how OSINT4Good is used across a variety of career fields and how you can get involved.

SpeakerBio: Nataly "someone_somewhere", Trace Labs

A cybersecurity professional obsessed with human psychology and making servers work how we expect them to, and a Trace Labs Director.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Welcome to the Voting Village

Tags: Voting Village | Creator Talk/Panel

When: Friday, Aug 7, 11:30 - 11:59 PDT

Where: LVCCW Level 2 W220 (Voting Village) (Voting Village Talks) - [Map](#)

Description:

The EIF Team and Staff will officially welcome our friends and guests to the Voting Village. We will give an overview of the content attendees should expect this year and the open questions we look forward to addressing.

Speakers: Brian DeMuth, Matt Blaze, Jake Braun, David Jefferson, Jeff Moss, Kendall Spencer, Philip Stark

SpeakerBio: Brian DeMuth

Brian DeMuth, a “former” hacker, is an entrepreneur and investor who has spent his 28-year career supporting the U.S. National Security Mission, cybersecurity businesses, and nonprofits. Brian is co-founder and General Partner of the Riphean Investments National Security Fund, a venture-studio-style investment fund focused on technology investments that strengthen national security for the U.S. and its citizens. He is the Founder of Immortal Cyber, Inc., an advanced cybersecurity research and engineering firm providing offensive cyber delivery services and “Cyber-as-a-Service” for unique clients, and Co-Founder & CEO of RapidAscent, Inc., a scalable, task-based cyber apprenticeship solution addressing the historic shortage of technical personnel in the U.S. and worldwide. Brian also co-founded and chairs the board of the Cyber Bytes Foundation, a 501(c)(3) dedicated to building a unique cyber ecosystem of educational and outreach programs for the cyber workforce. A longtime advocate for election security, Brian serves on the Board of Directors of the Election Integrity Foundation, the 501(c)(3) behind the DEF CON Voting Village.

SpeakerBio: Matt Blaze

Matt Blaze is the McDevitt chair in Computer Science and Law at Georgetown University, where he studies problems at the intersection of technology and public policy. Election systems and voting technology are central focuses of his research. He led teams as part of the California TTBR and Ohio EVEREST studies that each found deep and fundamental weaknesses in different election technologies used by those states and the rest of the US. He has testified on technical risks in elections before the US Congress and other bodies numerous times. Blaze is a co-founder of the Voting Village and president of the Election Integrity Foundation.

SpeakerBio: Jake Braun, DEF CON Franklin

Jake Braun is the co-founder of DEF CON Franklin and the Executive Director of the Cyber Policy Initiative at the University of Chicago Harris School of Public Policy. He most recently served in the White House as acting Principal Deputy National Cyber Director. While at the White House, he oversaw the implementation of the National Cybersecurity Strategy, including efforts to secure our water systems, modernize the federal cyber workforce, enhance cyber cooperation with allied nations, and develop AI cybersecurity policy.

In addition to his role at the University of Chicago, Mr. Braun co-founded the DEF CON Voting Machine Hacking Village. In that capacity, he co-authored two award-winning reports on the cyber security of our election infrastructure: the DEF CON 25 and 26 Voting Village Reports. Most recently, he partnered with DEF CON, the world's largest and longest running hacker conference, to launch “DEF CON Franklin,” a program to memorialize the most innovative and impactful findings from DEF CON in the annual “Hackers’ Almanack.” “DEF CON Franklin” also recruits cyber volunteers to support underresourced critical infrastructure.

SpeakerBio: David Jefferson

David Jefferson is an internationally recognized expert on voting systems and election technology, and an advisor to five successive California Secretaries of State. In 2004 he was coauthor of the SERVE Security Report detailing the security vulnerabilities in the Defense Department's proposed Internet voting system, leading to the cancellation of the program. In 2003 he was a member of the California Task Force on Touchscreen Voting, whose recommendations led to voter-verified paper audit trails for electronic voting machines. He has led half a dozen technical studies on reliability and security of voting systems, including the California Post-Election Audit Standards Working Group that produced the first government study of post-election auditing. He has served on the boards of directors of both the California Voter Foundation and Verified Voting, and is currently on the board of the Election Integrity Foundation that puts on the annual DEF CON Voting Village.

Dr. Jefferson received a BS in mathematics from Yale University, and a Ph.D. in computer science from Carnegie-Mellon University. From 1980 to 1994 he was a professor at the University of Southern California (USC) and then at UCLA. He is now retired from Lawrence Livermore National Laboratory where he conducted research in supercomputing and cyber security.

SpeakerBio: Jeff Moss

No BIO available

SpeakerBio: Kendall Spencer

Kendall Spencer is an attorney specializing in emerging companies, technology transactions, and the legal issues shaping innovation. Since joining DEF CON's Voting Village as a Georgetown Law student in 2019, he has worked alongside Matt Blaze, David Jefferson, and the Voting Village team at the intersection of election technology, cybersecurity, and democracy. Spencer serves on the Board of Directors of the Election Integrity Foundation and has advised state election officials on election security, post-election audits, and cybersecurity best practices. His work focuses on bridging the gap between technical research, public policy, and the law—helping policymakers, election officials, security researchers, and the public better understand the role election security plays in strengthening democratic institutions and public confidence in elections. A frequent DEF CON speaker, Spencer is passionate about fostering thoughtful, bipartisan conversations on the role of technology in protecting election integrity and the democratic principles that underpin a free and open society. Outside of his legal and technology work, Spencer is a rare book dealer and collector specializing in early American history and the Black diaspora.

SpeakerBio: Philip Stark

Philip B. Stark is Distinguished Professor of the Graduate School at the University of California, Berkeley, where he has served as department chair and associate dean. In 2007 he invented "risk-limiting audits" ("RLAs"), endorsed by the National Academies of Science, Engineering, and Medicine and the American Statistical Association, among others, and required or authorized by law in about 15 states. He designed and helped conduct the first dozen pilot RLAs, helped draft RLA legislation for several states, and has published open-source software to support RLAs. In 2012, he and David Wagner introduced "evidence-based elections," a paradigm for conducting demonstrably trustworthy elections. Stark has served on the Board of Advisors of the US Election Assistance Commission and its cybersecurity subcommittee, the Board of Directors of Verified Voting Foundation and the Election Integrity Foundation, and on the California Post Election Audit Standards Working Group. He has worked with the Secretaries of State of California, Colorado, and New Hampshire and numerous local election officials. He has testified about election integrity in state and federal courts and to legislators. He received the IEEE Cybersecurity Award for Practice, the UC Berkeley Chancellor's Award for Research in the Public Interest, and the John Gideon Award for Election Integrity. He is a fellow of the American Academy of Arts and Sciences, the American Statistical Association, and the Institute of Physics.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Welcome to your Airbnb, the key is under the mat -or- Alice and Bob with Padlocks

Tags: DCNextGen | Creator Event/Activity | Youth

When: Friday, Aug 7, 17:00 - 17:45 PDT

Where: LVCCW Level 3 W316 (DC NextGen) - [Map](#)

Description:

We teach everyone how to verify “there’s a padlock” but there’s a lot of cool math behind that padlock, and we will show, with everyday props and actors, how modern cryptography works under the hood. Can we implement Diffie-Hellman with padlocks? Instead of memorizing complicated math, we’ll solve puzzles together as a team and reveal how computers securely exchange secrets, protect private information, and prove someone’s identity online. Along the way, you’ll recreate the ideas behind the same technologies used by websites, games, banks, and messaging apps. Prerequisites: none. All props are provided and participants will keep some props.

SpeakerBio: Gilgamesh

No BIO available

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: What can those architecting agents learn from national security?

Tags: AI Village | Creator Talk/Panel

When: Saturday, Aug 8, 15:00 - 15:59 PDT

Where: LVCCW Level 1 Hall 2 603 (AI Village) - [Map](#)

Description:

This is a sit down discussion in a more casual conversational format:

The promise of agents is huge, but as the underlying LLMs get more capable, we are heading towards a future where a malicious or subverted agent cannot be contained through classical sandboxing approaches. The UK AISI's work on sandbox bench shows an agent doesn't even need to be malicious to attempt (and succeed) in breaking out of a regular sandbox. Looking to the future, approaches such as containerisation, based on Linux namespace separation, won't hold if the agent can find and exploit a novel kernel 0-day.

Remove the AI aspects, and the problem is that a workload might be able to find and exploit novel vulnerabilities, or evade even well-implemented controls. This is a problem the national security community has been working on for decades. This sort of defensive approach has only been necessary and justifiable to protect the most critical systems from the most capable adversaries, but in the near future, it may be needed to protect commodity systems from commodity attackers being enabled by AI.

This talk will cover some of the approaches that map to the challenge of securing agentic workloads and serve as a conversation starter for what previously niche thinking might become of commodity use.

SpeakerBio: David C Eight, UK NCSC AI Safety Institute

No BIO available

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: What Election Security Researchers Need to Know About the DMCA

Tags: Voting Village | Creator Talk/Panel

When: Friday, Aug 7, 10:30 - 10:59 PDT

Where: LVCCW Level 2 W220 (Voting Village) (Voting Village Talks) - [Map](#)

Description:

Section 1201 of the Digital Millennium Copyright Act (DMCA) has historically acted as a major legal barrier to election security research. Section 1201's "anti-circumvention" provision, 17 U.S.C. § 1201(a)(1), makes it illegal to circumvent or bypass a technological protection measure (TPM) that effectively controls access to a copyrighted work. Violations of the provision can carry both civil and criminal liability, making it a serious risk. Statutory exemptions for security testing, 17 U.S.C. § 1201(j), and encryption research, 17 U.S.C. § 1201(g), apply in some instances, but have important limitations. The security testing exemption covers "good faith" security testing, provided that the research has been authorized by the owner of the computer, and does not violate other laws like the Computer Fraud and Abuse Act or the Copyright Act. The encryption research exemption covers the investigation of encryption applied to copyrighted works, so long as those works were lawfully obtained, and the researcher has made a "good faith effort to obtain authorization." Section 1201 has historically had a substantial chilling effect on election security research even with these statutory exemptions in place. To address this problem, U.S. regulators adopted a much broader "temporary" security research exemption that provides stronger protection for critical security research on voting machines. The current version of the temporary exemption, 37 C.F.R. § 201.40(b)(18), covers "good faith security research" on a "lawfully acquired" computer, or with the permission of the owner. The temporary exemption enables security research without the need for permission from voting machine companies. However, risks remain despite the temporary exemption, which contains ambiguities and loopholes that voting machine companies sometimes exploit. This talk will explain what the exemption covers, what it may not, and why it is so important to the research that keeps our elections safe and secure.

SpeakerBio: Tori Noble

Tori Noble is a Staff Attorney at the Electronic Frontier Foundation specializing in free speech, intellectual property, cybersecurity, and artificial intelligence issues. Tori litigates cases and files amicus briefs in state and federal courts. Representative cases include defending online publishers from lawsuits intended to silence their work; advancing transparency into government activities that harm digital rights; and advocating against overbroad interpretations of copyright laws in AI cases. Tori also advises security and encryption researchers through EFF's Coder's Rights Project. Tori co-leads EFF's policy work on cybersecurity and AI. Prior to joining EFF, Tori represented media companies, television and film producers, and journalists as a litigation associate at Dentons US LLP and a First Amendment fellow at The Intercept. Tori holds a B.A. from the University of Michigan Gerald R. Ford School of Public Policy and a J.D. from Stanford Law School. Tori holds a B.A. from the University of Michigan Gerald R. Ford School of Public Policy and a J.D. from Stanford Law School.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: What Got You Here Won't Get You There: Security in the AI Era

Tags: Middle Easterns & Africans in Cyber Security (MEACS) | Creator Talk/Panel

When: Friday, Aug 7, 17:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 4 1306 (Middle Easterns & Africans in Cyber Security (MEACS) Community) - [Map](#)

Description:

A candid panel on how AI is reshaping security careers. We sit down with practitioners ranging from CISO to product security engineer, working across governance, physical hardware and SaaS, for an honest 45-minute conversation about what it takes to break in, level up, and stand out now that AI is changing what skills matter, what roles look like, and how hiring gets done.

SpeakerBio: Amber Bennoui

No BIO available

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

AI Village - Saturday - 11:00-11:59 PDT

Title: What is AI? Interactive, Unplugged Activity

Tags: AI Village | Creator Event/Activity

When: Saturday, Aug 8, 11:00 - 11:59 PDT

Where: LVCCW Level 1 Hall 2 603 (AI Village) - [Map](#)

Description:

Ever wonder what's actually happening inside an AI? In this hands-on, no-screens-required workshop, you'll build your own neural network out of flashcards and pipe cleaners, "train" it, and watch it try (and sometimes fail!) to answer prompts. You'll grow your model, give it tools and skills, and then turn the tables: try out real attacks like prompt injection, tool misuse, and data poisoning, and learn the defenses AI security researchers use to stop them, like containerization. No coding or experience required, just curiosity!

SpeakerBio: Sam Mosley, CodeBloom

No BIO available

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

AI Village - Sunday - 11:00-11:59 PDT

Title: What is AI? Interactive, Unplugged Activity

Tags: AI Village | Creator Event/Activity

When: Sunday, Aug 9, 11:00 - 11:59 PDT

Where: LVCCW Level 1 Hall 2 603 (AI Village) - [Map](#)

Description:

Ever wonder what's actually happening inside an AI? In this hands-on, no-screens-required workshop, you'll build your own neural network out of flashcards and pipe cleaners, "train" it, and watch it try (and sometimes fail!) to answer prompts. You'll grow your model, give it tools and skills, and then turn the tables: try out real attacks like prompt injection, tool misuse, and data poisoning, and learn the defenses AI security researchers use to stop them, like containerization. No coding or experience required, just curiosity!

SpeakerBio: Sam Mosley, CodeBloom

No BIO available

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: What is AI?

Tags: CodeBloom | Creator Workshop

When: Saturday, Aug 8, 16:00 - 16:59 PDT

Where: LVCCW Level 1 Hall 4 1304 (CodeBloom Community) - [Map](#)

Description:

Curious what is actually happening inside an AI when it answers your questions? In this session, you'll build your very own neural network using flashcards and pipe cleaners, test it out with tricky prompts, and watch what happens when you grow it bigger, just like real AI companies do! We'll also talk about how AI models pick up new skills, some of the sneaky ways people try to trick AI, and the clever ways researchers keep AI safe. A fun, hands on way to learn about AI for curious minds of all levels. If you've ever wanted to get involved in our community or teach our classes, this would be a great time to stop by and learn more!

SpeakerBio: Sam Mosley, CodeBloom

No BIO available

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: What is AI?

Tags: CodeBloom | Creator Workshop

When: Friday, Aug 7, 16:00 - 16:59 PDT

Where: LVCCW Level 1 Hall 4 1304 (CodeBloom Community) - [Map](#)

Description:

Curious what is actually happening inside an AI when it answers your questions? In this session, you'll build your very own neural network using flashcards and pipe cleaners, test it out with tricky prompts, and watch what happens when you grow it bigger, just like real AI companies do! We'll also talk about how AI models pick up new skills, some of the sneaky ways people try to trick AI, and the clever ways researchers keep AI safe. A fun, hands on way to learn about AI for curious minds of all levels. If you've ever wanted to get involved in our community or teach our classes, this would be a great time to stop by and learn more!

SpeakerBio: Sam Mosley, CodeBloom

No BIO available

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: What is AI?

Tags: CodeBloom | Creator Workshop

When: Friday, Aug 7, 13:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 4 1304 (CodeBloom Community) - [Map](#)

Description:

Curious what is actually happening inside an AI when it answers your questions? In this session, you'll build your very own neural network using flashcards and pipe cleaners, test it out with tricky prompts, and watch what happens when you grow it bigger, just like real AI companies do! We'll also talk about how AI models pick up new skills, some of the sneaky ways people try to trick AI, and the clever ways researchers keep AI safe. A fun, hands on way to learn about AI for curious minds of all levels. If you've ever wanted to get involved in our community or teach our classes, this would be a great time to stop by and learn more!

SpeakerBio: Sam Mosley, CodeBloom

No BIO available

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: What is AI?

Tags: CodeBloom | Creator Workshop

When: Sunday, Aug 9, 13:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 4 1304 (CodeBloom Community) - [Map](#)

Description:

Curious what is actually happening inside an AI when it answers your questions? In this session, you'll build your very own neural network using flashcards and pipe cleaners, test it out with tricky prompts, and watch what happens when you grow it bigger, just like real AI companies do! We'll also talk about how AI models pick up new skills, some of the sneaky ways people try to trick AI, and the clever ways researchers keep AI safe. A fun, hands on way to learn about AI for curious minds of all levels. If you've ever wanted to get involved in our community or teach our classes, this would be a great time to stop by and learn more!

SpeakerBio: Sam Mosley, CodeBloom

No BIO available

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: What is AI?

Tags: CodeBloom | Creator Workshop

When: Saturday, Aug 8, 13:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 4 1304 (CodeBloom Community) - [Map](#)

Description:

Curious what is actually happening inside an AI when it answers your questions? In this session, you'll build your very own neural network using flashcards and pipe cleaners, test it out with tricky prompts, and watch what happens when you grow it bigger, just like real AI companies do! We'll also talk about how AI models pick up new skills, some of the sneaky ways people try to trick AI, and the clever ways researchers keep AI safe. A fun, hands on way to learn about AI for curious minds of all levels. If you've ever wanted to get involved in our community or teach our classes, this would be a great time to stop by and learn more!

SpeakerBio: Sam Mosley, CodeBloom

No BIO available

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: What is the Right Balance of Rules for Defenders & Adversaries? Determining which dual-use model restrictions make sense and which only disarm defenders

Tags: DEF CON Official Talk | AI Village

When: Friday, Aug 7, 13:30 - 14:59 PDT

Where: LVCCW Level 1 Hall 3 1006 (Main Track 1) - [Map](#)

Description:

Defenders and attackers are locked in a renewed race where AI has enabled new defenses and new attacks. In this iterated dual-use, game-theoretic situation, how can defenders be maximally enabled without unduly increasing the risks that adversaries get access to the same capabilities?

As highly capable LLMs face increasing restrictions and regulatory interest from policy makers, adversaries are attempting to evade restrictions, sometimes putting those who play by the rules at a disadvantage.

This panel will discuss recent examples and will look toward the near future as model capabilities increase yet again in both closed and open weights models.

Speakers: Emanuel Gawrieh, Jason Clinton, Bruce Schneier, Heather Adkins

SpeakerBio: Emanuel Gawrieh, Co-Chair at AI Village

Emanuel Gawrieh is a Senior Chaos Containment Engineer on the Advanced Threat Protection team at Google, where he specializes in architecting and proving out threat models for complex workloads in highly regulated environments. As a core member of Google's Secure AI Framework (SAIF) team, he works closely with Google AI Red Team, Google DeepMind, and the Cloud CISO's office to establish AI security standards - contributing to the early development and specialized fine-tuning of dual-use models like SecGemini to mitigate emerging AI-specific risks. Outside of his work at Google, he is a leading voice in AI Security policy and community evangelism - having presented at DEFCON, RSA and is an active member of the [un]prompted CFP board. Additionally, he has architected the infrastructure for several Generative AI Red Team events and actively advises congressional leaders on AI and cybersecurity policy.

SpeakerBio: Jason Clinton, Deputy CISO at Anthropic

Jason joined Anthropic in April 2023 as its first CISO after more than a decade at Google, where he most recently led Chrome infrastructure security working on defense against advanced persistent threats. While at Google, he also worked on ChromeOS and Android Pay. At Anthropic, Jason guides security strategy including detection and response, compliance, physical security, security engineering and IT. Jason promotes the security organization's work to uphold Anthropic's Responsible Scaling Policy framework, ensuring that the company has appropriate security safeguards in place for the responsible development and deployment of AI models. He is also the author of "Ruby Phrasebook".

SpeakerBio: Bruce Schneier, Advisory Board Member at VerifiedVoting.org

Bruce Schneier is an internationally renowned security technologist, called a "security guru" by the Economist. He is the New York Times best-selling author of 14 books – including *Rewiring Democracy* and *A Hacker's Mind* -- as well as hundreds of articles, essays, and academic papers. His long-running newsletter and blog, "Schneier on Security," is one of the most popular sources of cybersecurity news on the internet. Schneier is a Fellow and Lecturer in Public Policy at the Harvard Kennedy School and the Munk School at the University of Toronto. He is a fellow at the Berkman-Klein Center for Internet and Society at Harvard University, a board member of the Electronic Frontier Foundation and AccessNow, and an advisory board member of EPIC and VerifiedVoting.org. He is also the Chief of Security Architecture at Inrupt, Inc.

SpeakerBio: Heather Adkins, Vice President of Security Engineering at Google

Heather Adkins is a 24-year Google veteran and founding member of the Google Security Team. As VP, Security Engineering and head of Google's Office of Cybersecurity Resilience she has built a global team responsible for maintaining the safety and security of Google's networks, systems and applications. She has an extensive background in practical security, and has worked to build and secure some of the world's largest infrastructure. She is co-author of *Building Secure and Reliable Systems* (O'Reilly, 2020), was deputy chair of CISA's Cyber Safety Review Board, and has advised numerous organizations on how to adopt modern defendable architectures.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: What Scammers Know That Social Engineers Don't: Three Techniques for Tough Cases

Tags: Social Engineering Community Village | Creator Talk/Panel

When: Saturday, Aug 8, 15:30 - 15:59 PDT

Where: LVCCW Level 3 W317-319 (Social Engineering Community Village) - [Map](#)

Description:

Most social engineering training teaches techniques that exploit emotional triggers like urgency, fear, or flattery. But what happens when the target has been trained to spot these and they are on high alert? In this talk I will demonstrate three techniques I've learned from studying career scammers for my research at F-Secure, and I'll show you how to apply them to your social engineering operations. All three of these techniques work specifically for targets who have been already primed against falling for scams and other social engineering exploits. In other words, these are techniques designed for your tough cases. First, I'll demonstrate Awareness Hijacking, where the operator uses the target's knowledge of one scam to trap them in a different one. Then I'll show Complexity-as-Crucible, where the operator engineers a scenario that lets them become the target's trusted guide. Finally, I'll demonstrate the First Win, where the operator purposely lets the target "beat the scam" without realizing they've actually entrapped themselves. Participants will leave with three new techniques that are directly applicable to red team social engineering engagements where the targets may be on high alert or trained against falling for more traditional manipulation techniques.

SpeakerBio: Megan Squire, Principal Threat Intelligence Researcher at F-Secure

Dr. Megan Squire is a Principal threat intelligence researcher at F-Secure, where she studies AI safety, scams, and fraud. Before moving into threat intel, she spent over a decade studying online recruitment, illicit finance, and adversary networks in the domestic violent extremism domain. Her work on threat intelligence and OSINT has been featured in WIRED, The New York Times, PBS-Frontline, The Washington Post, and Dark Reading.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: What TEEs Do Not Hide: Residual Metadata Leakage in Confidential LLM Serving

Tags: Crypto & Privacy Village | Creator Talk/Panel

When: Friday, Aug 7, 10:30 - 10:59 PDT

Where: LVCCW Level 1 Hall 3 1105 (Creator Stage 3) - [Map](#)

Description:

Confidential LLM inference protects prompt, model, KV-cache, and intermediate-tensor memory, but it does not remove the metadata emitted by the serving stack. We audit those emitted surfaces on a verified H100 confidential-GPU serving setup using a dense/MoE Gemma pair. The claim is narrow: we do not show a TEE memory break, and corrected client timing does not support a leakage claim. We do show that client/proxy-observed HTTP-stream metadata and low-concurrency pre/post-scrape metrics reveal request attributes in this harness. Decomposition ties the signal to exported token counters, request bytes, response bytes, and application-level stream-chunk shape. Deployed mitigations suppress those carriers: token-counter redaction reduces metrics leakage, request padding removes the direct prompt-length row, and chunk padding suppresses the tested HTTP-stream rows. Memory confidentiality and metadata minimization are different properties, and confidential LLM serving needs both.

SpeakerBio: Anup Swamy Veena

I am a security researcher and engineer focused on cryptography, privacy, and AI systems. My work spans zero-knowledge proofs, trusted execution environments (TEEs), confidential computing, and secure distributed infrastructure, with a particular interest in building verifiable and privacy-preserving AI. Over the years, I have contributed to open-source cryptography projects in the Rust ecosystem and worked on cryptographic protocols, proving systems, and decentralized infrastructure. Currently, I focus on secure AI inference in TEE and attestations, verifiable computation, and the security of large-scale AI deployments, including research on metadata leakage in confidential AI systems and routing leakage in Mixture-of-Experts models. My interests lie in applying cryptographic techniques to build trustworthy systems at the intersection of security, distributed systems, and machine learning.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: What we learned from SATAN about the MYTH of Mythos

Tags: AI Village | Creator Talk/Panel

When: Saturday, Aug 8, 14:00 - 14:30 PDT

Where: LVCCW Level 1 Hall 3 801 (Creator Stage 2) - [Map](#)

Description:

Thirty years ago a new and powerful (at the time) vulnerability scanner burst onto the scene. SATAN (System Administrators Tool for Analyzing Networks) sparked controversy by putting advanced network reconnaissance capabilities into the hands of ordinary defenders. Critics warned it would empower attackers and was, therefore, too dangerous to release publicly. In fact, it helped accelerate security awareness and improve defensive practices. Today, AI-powered security platforms such as Mythos face similar calls for restriction. This talk examines the lessons of SATAN and argues that limiting access to powerful security tools rarely stops capable adversaries, but often disadvantages defenders, researchers, and educators. As the security community debates AI's future, history offers a valuable reminder: broad access to defensive capability has often strengthened security more than secrecy.

SpeakerBio: Jeff Crume

Jeff Crume is an IBM Distinguished Engineer and Master Inventor with more than 40 years' experience in the IT industry. He has a PhD in Cybersecurity and serves as an Adjunct Professor at NC State University. Jeff's YouTube videos have been viewed more than 25 million times and he is the author of a book entitled "Inside Internet Security: What Hackers Don't Want You To Know" as well as a contributing author to the "Information Security Management Handbook." He is a member of the inaugural class of the NC State University Computer Science Alumni Hall of Fame and serves on the editorial board for the "Information and Computer Security" research journal. Jeff lived in Beijing on assignment in 2006 and has worked with clients in 50 countries.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: What Your Coding Agent Did Last Night: Runtime Security for AI Coding Agents

Tags: Intermediate | AppSec Village | Creator Talk/Panel

When: Saturday, Aug 8, 11:10 - 11:40 PDT

Where: LVCCW Level 1 Hall 2 604 (Appsec Village) Main Stage - [Map](#)

Description:

Your coding agent ran 200 tool calls last night. File reads, shell commands, network requests, all with your permissions, mostly invisible. Today's defenses miss the attacks landing now: MCP tool poisoning, prompt injection via repo content, and credential-exfiltration chains where only the sequence is malicious.

I'll present AgentsLeak, an open-source runtime monitor that hooks Claude Code and Cursor at the tool-call boundary and blocks before execution. Live demo: session telemetry showing the calls the agent made versus the calls it disclosed, and behavioral chain detection catching multi-step exfiltration.

SpeakerBio: Inga Cherny

Inga Cherny is an ML Researcher at CrowdStrike specializing in AI security, LLM vulnerabilities, adversarial ML, and prompt injection defenses.

Previously, she was a security researcher at Cato Networks and a member of Cato CTRL, focusing on emerging threats, offensive and defensive security research.

With a decade of experience spanning security and applied machine learning, Inga focuses on uncovering new attack vectors and building more resilient AI and security systems.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: What's Behind the Curtain? Tearing Down AWS's AI Agent Runtime From the Inside

Tags: Cloud Village | Creator Talk/Panel

When: Saturday, Aug 8, 13:30 - 14:10 PDT

Where: LVCCW Level 3 W313 (Cloud Village Talks) - [Map](#)

Description:

How much do you actually know about one of the world's leading agent-building platforms? When you deploy an AI agent to Bedrock AgentCore, your code lands inside a Firecracker microVM - and you're told almost nothing about what's in there with you. So I decided to find out.

Starting from nothing, we'll work our way through the layers: Runtime, Networking, Identity, Observability, etc - mapping what an attacker can reach, what they can break, and what actually holds. We'll explore novel techniques that allowed me to extract information the platform was never meant to expose.

Along the way, we'll uncover an undocumented platform, strange auth behaviors, security boundaries that didn't hold up, and internal architecture details not covered in any public documentation.

By the end, you'll see what's really behind the curtain and what it tells us about how AWS builds and secures managed AI workloads. The methodology is reusable - the next time you're researching an opaque managed runtime, you'll know where to look.

SpeakerBio: Dan Gansel

Dan Gansel is a cloud security specialist with deep expertise in cloud API research, secure cloud solutions and architecture design. Dan has led cloud security research teams and has a track record of uncovering novel attack techniques in cloud environments. As a Security Researcher at Upwind Security, Dan continues to push the boundaries of cloud security, focusing on uncovering blind spots in the services organizations trust the most.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: When AI Finds Everything: Vulnerability Policy for the Coming Discovery Surge

Tags: Policy @ DEF CON | Creator Talk/Panel

When: Friday, Aug 7, 15:30 - 16:30 PDT

Where: LVCCW Level 2 W210-211 (Policy Village) - [Map](#)

Description:

AI-enabled vulnerability discovery is moving from novelty to inevitability. As frontier systems become better at finding, validating, and reporting vulnerabilities at scale, the ecosystem will face a basic policy question: what happens when discovery accelerates faster than coordination, triage, remediation, prioritization, and response can absorb? This talk examines the policy and operational implications of a world where vulnerability discovery becomes cheaper, faster, and more automated. Using CVE, CWE, CNA operations, and CISA's vulnerability management mission as grounding examples, we will explore how current processes may strain under higher volume, probabilistic findings, duplicate reports, inconsistent quality, and incomplete downstream impact context. The talk will not argue that AI breaks vulnerability management. Instead, it argues that AI magnifies existing gaps across the software development lifecycle and incident response ecosystem: unclear responsibility, uneven data quality, insufficient automation, fragile public-good infrastructure, and policy models that often assume human-scale discovery, reporting, and response. We will discuss what policymakers, program stewards, hackers, vendors, software producers, defenders, and infrastructure operators should do now to prepare for the next era of vulnerab

Speakers: Alec Summers, Lindsey Cerkovnik, Madison Ficorelli

SpeakerBio: Alec Summers, The MITRE Corporation

Alec Summers is a principal cybersecurity engineer at the MITRE Corporation with diverse and extensive experience in software assurance and vulnerability management, as well as cyber operations, assessments, and supply chain risk management. He is the MITRE CVE and CWE Project Leader, managing teams that support vulnerability and weakness research & analysis, content production, program coordination, services development, and community engagement across a global partner base comprising industry, government, and academia. He serves as the moderator for the CVE Board and CWE Board.

SpeakerBio: Lindsey Cerkovnik, CISA

Lindsey Cerkovnik is the Chief of CISA's Vulnerability Response & Coordination (VRC) Branch. Her team is responsible for CISA's Coordinated Vulnerability Disclosure (CVD) process, the Known Exploited Vulnerabilities (KEV) catalog, and CISA's Stakeholder Specific Vulnerability Categorization (SSVC) process. Lindsey and her team help to maintain, support, and advance the global vulnerability ecosystem by funding and overseeing the CVE and CVE Numbering Authority (CNA) programs, leading the production and dissemination of machine-readable vulnerability enrichment information, and engaging in valuable technical collaboration with the vulnerability research community.

SpeakerBio: Madison Ficorelli

Madison Ficorelli is a vulnerability transparency advocate and staff security manager at GitHub, leading the advisory database curation team. She is passionate about vulnerability reporting, response, and disclosure, and co-chairs the relevant Open Source Security Foundation (OpenSSF) working group and serves on the CVE Program Board. Her views are enriched by her prior experience as a product incident response analyst at GitHub and as a vulnerability coordinator at the CERT Coordination Center at the Software Engineering Institute at Carnegie Mellon University.



Title: When Cash Runs on Windows: A Red Team Look at ATM Attack Surfaces

Tags: La Villa Community | Creator Talk/Panel

When: Saturday, Aug 8, 14:30 - 15:30 PDT

Where: LVCCW Level 1 Hall 4 1416 (La Villa Community) Main Stage - [Map](#)

Description:

Muchos cajeros automáticos siguen siendo, en esencia, computadoras Windows especializadas. Algunos son modernos, otros llevan años operando con sistemas heredados, configuraciones antiguas y controles que nunca fueron revisados a profundidad. Están en gasolineras, supermercados y esquinas, conectados a infraestructura crítica donde una mala decisión de hardening, segmentación o administración remota puede convertirse en un riesgo real.

Nadie los toca. Nadie los cuestiona. Hay dinero adentro.

Esta charla resume hallazgos de ejercicios reales de pentesting sobre ATMs realizados en América Latina. Veremos cómo se ve la seguridad ATM en producción: qué controles suelen estar presentes, cuáles fallan de formas inesperadas y cómo debilidades aparentemente menores pueden encadenarse hasta comprometer infraestructura crítica.

Entre los hallazgos analizaremos fallas en controles de endpoint, hardening, segmentación, administración remota y exposición de servicios legacy. También veremos qué controles resistieron, por qué lo hicieron y qué diferencia a un ATM correctamente endurecido de uno que puede convertirse en punto de entrada hacia infraestructura crítica bancaria.

Más que mostrar “cómo atacar un cajero”, esta charla busca crear conciencia sobre la importancia de endurecer y monitorizar estos equipos.

SpeakerBio: Gerardo Mejia, Red Teamer

Es especialista en ciberseguridad ofensiva, con enfoque en operaciones de red teaming, purple teaming, pruebas de penetración, campañas avanzadas de phishing y ataques dirigidos a entornos de Active Directory. Actualmente forma parte del un equipo regional de seguridad ofensiva, donde diseña y ejecuta ejercicios de simulación de adversarios para fortalecer la resiliencia de las organizaciones ante amenazas sofisticadas.

Cuenta con certificaciones destacadas, como CRTO, CRTP, PNPT, eWPT, CR (HTB Ambassador), C-ADPenX y eCCPT.

Ha sido conferencista en eventos internacionales como PWNEDCR en Costa Rica, BSides Panamá, Dojo Conf Panamá, HackConRD en República Dominicana y Ekoparty en Argentina, Defcon 33 La Villa, Kavacon

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: When Machines Attack Machines: Detecting AI-Autonomous Cloud Compromise at NHI Scale

Tags: Cloud Village | Creator Talk/Panel

When: Sunday, Aug 9, 10:40 - 11:20 PDT

Where: LVCCW Level 3 W313 (Cloud Village Talks) - [Map](#)

Description:

Two forces are converging to break cloud detection as we know it. First, non-human identities (NHIs) such as service accounts, API keys, OAuth tokens, AI agent credentials now outnumber human identities by ratios exceeding 100:1 in enterprise environments. 97% of these NHIs carry excessive privileges, 71% are never rotated within recommended timeframes, and over 40% are orphaned with no human owner. Second, attackers have begun using AI agents to compromise these identities at machine speed, performing hundreds of reconnaissance actions per minute, autonomously mapping privilege escalation paths, and executing lateral movement faster than any human analyst can respond. The result is a detection problem that traditional security tools were never designed to handle: machine-speed attacks against machine identities, where the attacker's AI agent looks indistinguishable from the defender's AI agent in the logs. This talk presents the first detection engineering framework purpose-built for this collision covering how to baseline NHI behavior, detect AI-autonomous compromise patterns, and build response automation that can match attacker speed.

SpeakerBio: Gowthamaraj Rajendran

Gowthamaraj Rajendran is a Detection and Response Engineer at Meta with over 6 years of experience in cybersecurity. He specializes in building high-fidelity rules and improving detection engineering practices at scale.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Blacks In Cyber Village - Friday - 12:00-12:25 PDT

Title: When the Agent Lies: Why Neurosymbolic AI is the Security Layer Nobody is Building Yet

Tags: Blacks In Cyber Village | Creator Workshop

When: Friday, Aug 7, 12:00 - 12:25 PDT

Where: LVCCW Level 3 W322-W324 (BIC Village) - [Map](#)

Description:

AI agents are being handed the keys to enterprise infrastructure, executing code, querying databases, making access decisions, and increasingly controlling physical systems. Most are built on pure LLM inference, making them stochastic, opaque, and vulnerable in ways traditional security tooling was never designed to catch. This session breaks down how LLM-based agent architectures fail from a security perspective, what a more auditable architecture looks like in practice, and why the security community needs to be driving this conversation before the agents are already inside the perimeter. Discover how grounding agent decisions in structured knowledge graphs, symbolic reasoning, and auditable state transitions dramatically reduces this exposure, offering a critical new security layer. Join us to understand the future of secure AI agents.

SpeakerBio: Maureese Williams, Senior LLM and Data Engineer

Maureese Williams is a Senior LLM and Data Engineer with extensive experience in media, finance, and technology. They specialize in leveraging AI and Large Language Models (LLMs) to solve real-world problems and empower developers. Their background includes working with companies like Warner Bros Discovery, Accenture, Ugam, Vanguard, and BlackRock, focusing on data engineering, vector databases, and generative AI. Maureese is also known for contributing to open-source projects.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Adversary Village - Friday - 17:15-17:59 PDT

Title: Where hackers find their people, and security finds its strength

Tags: Adversary Village | Creator Talk/Panel

When: Friday, Aug 7, 17:15 - 17:59 PDT

Where: LVCCW Level 1 Hall 3 1105 (Creator Stage 3) - [Map](#)

Description:

Before it was an industry, this was just people. Curious folks poking at things, breaking stuff to figure out how it worked, and telling the next person what they found. Somewhere along the way a few of them started building the rooms where that could happen: the cons, the villages, the meetups, the spaces where you finally found your crew.

This panel gets some of those organizers together to talk about something we don't say out loud enough: the community is the security. Every mentor who answered your dumb questions, every village that felt like home, every hallway conversation that turned into a tool or a job or a friendship, someone had to make space for that. We will swap stories about what it takes to build and protect these communities, why the people who show up matter more than anything, and how the spaces we create end up being some of the strongest defense we have got. Pull up a chair. Nobody does this alone, and that is the whole point.

Speakers: Seeyew Mo, Ashley S, Tatiana U, Heidi Potter, Christine Billingsley

SpeakerBio: Seeyew Mo, Director of Training for DEF CON.

Seeyew Mo is the Senior Advisor for Cyber Maryland where he leads the state's cyber workforce development. He also serves as the Director of Training for DEF CON. He previously served as the Assistant National Cyber Director for Cyber Workforce, Training and Education at the Office of National Cyber Director (ONCD). In his role, Seeyew leads and coordinates the implementation the White House's National Cyber Workforce and Education Strategy. He believes in taking a holistic view – doctrine, people, and technology - to making advancements in cyber workforce and digital safety awareness. Seeyew is an expert in the intersection of cybersecurity, technology, and national security with 18 years of experience spanning tech development, policymaking, and political campaigning.

SpeakerBio: Ashley S, Sr. Solutions Engineer at Censys

Ashley is a cybersecurity researcher, threat intelligence practitioner, and Senior Sales Engineer at Censys, where she conducts strategic research on IoT botnets and adversarial infrastructure. Her research sits at the intersection of hardware-based attack infrastructure and influence operations, tracking how low-cost consumer electronics are weaponized as residential proxy networks, ad fraud engines, and persistent footholds inside homes and enterprise networks. She spends tons of time building up the cybersecurity community and got her start by volunteering after making a career pivot after her military service. She is very passionate about community protection and community building, as evidenced by her role as Chief Security Officer for BsidesLV.

SpeakerBio: Tatiana U, Technical Program Manager at Bugcrowd

Tatiana (Tati) is the Technical Program Manager for Live Hacking at Bugcrowd, which means she's usually the one making sure a room full of hackers actually turns into a working event. She didn't come up in this industry through school or a straight career path. She came up through it the way most people do: somebody let her in, answered her questions, and made room for her at the table. She's spent the years since returning the favor.

SpeakerBio: Heidi Potter, Chief Operating Officer at Turngate

Heidi Potter has spent much of her career bringing people together. Best known for her twenty years helping build and run ShmooCon, she remains passionate about creating welcoming spaces where people can learn, connect, and share ideas. She

currently serves as COO of Turngate and spends her free time walking, biking, and occasionally embracing carefully managed chaos.

SpeakerBio: Christine Billingsley, Chief Operating Officer at Military Cyber Professionals Association

Christine Billingsley is the Chief Operating Officer at the Military Cyber Professionals Association. An accomplished operations and marketing professional with a proven track record of innovation and delivery of best-in-class projects, experiences, and events. She is the creator of the DEF CON Arcade Party and author of Cyber Snackz, an introductory cybersecurity activity book centered around a team of adorable animals who work in different areas of cybersecurity. She is passionate about getting today's youth interested in cyber. She is a mom to humans and a spunky Pomeranian.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Where the Authorization Boundary Goes in Agent Workflows

Tags: Middle Easterns & Africans in Cyber Security (MEACS) | Creator Talk/Panel

When: Sunday, Aug 9, 12:00 - 12:59 PDT

Where: LVCCW Level 1 Hall 4 1306 (Middle Easterns & Africans in Cyber Security (MEACS) Community) - [Map](#)

Description:

In May 2026, attackers took over high-profile Instagram accounts by asking Meta's AI support assistant to change a recovery email. The agent changed it, the attacker used the recovery flow, and the account was gone. The agent was not tricked in any exotic way. It just did something it was allowed to do, for someone who should not have been allowed to ask.

I have spent a while delivering agentic AI security work, and I keep seeing the same thing. Everyone is struggling to push authorization into AI agents. Teams deploy an agent and cannot actually tell you what it is capable of or what rules it is bound by. This is the identity and access management problem we have been fighting for decades, now behind a conversational interface. The agent looks like a smart assistant, but it can act like an admin, and nobody drew the line for what it is allowed to reach.

Maze is the pattern I came up with for this, and I have implemented it and it works. The agent never executes directly. Its request enters a fixed sequence of gates: is this a privileged action, is the user authenticated, do they own the target account, can this tool mutate data, does policy allow it, is it within rate limits, did step-up verification pass. Each gate either advances the request or drops it into a blocked state, and there is exactly one path through to execution. Every outcome, pass or block, is written to an audit log. The authorization does not live inside the model, where it can be talked around. It lives in the gates, and the agent cannot route around them.

I will walk through the Meta case as the example, then show how Maze structures the workflow so the agent stays inside gates it cannot step past.

SpeakerBio: Mohamed Magdy AbuMuslim

No BIO available

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Ham Radio Village - Friday - 14:30-15:10 PDT

Title: Who Owns Your Shack? Open Source, Amateur Radio, and the Software We Can't Afford to Lose

Tags: Ham Radio Village | Creator Talk/Panel

When: Friday, Aug 7, 14:30 - 15:10 PDT

Where: LVCCW Level 3 W315 (Ham Radio Village) - [Map](#)

Description:

A 30–40 minute talk for Ham Radio Village at Defcon. Primary audience is licensed amateur radio operators, with a secondary audience of hackers and security-minded attendees unfamiliar with the hobby. The talk uses the post-mortem license failure pattern in amateur radio software as motivating context, builds an ownership/self-reliance argument, and presents open-packet as a working existence proof of the open-source alternative.

You own your radio. The protocols you use — AX.25 and APRS — are open standards anyone can implement. But the software your club depends on? That's often a different story.

For the security-minded: this is a story about critical communication infrastructure running on software whose source code doesn't exist.

Amateur radio has a long tradition of self-reliance: building your own antennas, maintaining your own gear, understanding your own stack. That tradition breaks down at the software layer. Too much of the tooling that holds the hobby together is maintained by a single developer, distributed as a closed binary, with no source code and no succession plan. We've already seen what happens when that developer is gone: When Roger Barker G4IDE passed in 2004, UI-View32's source code went with him — leaving the community to maintain unofficial workarounds rather than fix the underlying binary, with the registration servers eventually going dark. Bob Bruninga WB4APR's death in 2022 raised the same question for his reference APRS implementations and the aprs.org site he maintained. These aren't edge cases — they're a pattern, and the hobby's aging demographics make it one we can't ignore.

This talk makes the case that open-source licensing isn't just a software philosophy — it's an infrastructure resilience strategy. If a tool is critical to your club's operations or your emergency net, its source code needs to outlive its author.

As a working example, we'll look at open-packet: an early-stage, MIT-licensed packet messaging client in Python — a working existence proof that the open-source path is viable. A brief live demo will show the basic functionality, along with some nice to have extras such as visual themes and a web client.

Attendees will leave with a concrete lens for evaluating the software they depend on, a GitHub link, and three specific asks — from "try it" to "apply this thinking to every tool in your shack."

SpeakerBio: Jeremy Banker - K0JLB

Bio: Jeremy Banker is a Senior Security Software Engineer at Horizon3.ai, focused on the reliability and resiliency of Horizon3's automated penetration testing platform. He previously spent nearly a decade at VMware, where he co-founded the Security Product Engineering group and led efforts to secure VMware's software supply chain. His open source security tooling, including Build Inspector for CI/CD pipeline anomaly detection and Tommyknocker for automated security control validation, has been featured at Black Hat Arsenal and DEF CON Demo Labs. A licensed amateur radio operator since 2010, he built open-packet, an MIT licensed Python client for packet messaging, after becoming frustrated with the existing closed-source options.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Whose Agent Is It Anyway? Agency, Authorization, and Accountability in the Year of the AI Agent

Tags: Policy @ DEF CON | Creator Talk/Panel

When: Saturday, Aug 8, 10:00 - 10:59 PDT

Where: LVCCW Level 1 Hall 3 801 (Creator Stage 1) - [Map](#)

Description:

DEF CON 34's theme is Agency—as in digital self-determination. This is also the year agentic AI went mainstream. Those two meanings of “agency” are now colliding in the legal sphere, and early answers are not in the user's favor. A federal court ruled that a user's instruction to her own AI agent to access her own Amazon account may violate federal cybercrime law—because the platform, not the user, controls authorization. The decision is up for appeal. Meanwhile, the market is trending the same way: agents go where B2B agreements permit. The web, as navigated by AI agents, is becoming a permission graph between companies. The instinct is clear: the user's delegation should count, agents should go where the user can. But the question is harder than it looks. Real vulnerabilities allow agents inside authenticated platform environments to be hijacked. Platforms cannot secure these agents or distinguish them from legitimate user sessions. When the user delegates, she opens channels an attacker can redirect. The platform must decide whether to accept the risk of tools it didn't build operating in spaces it's responsible for protecting. Neither courts nor markets are producing the right answer. Two cybersecurity lawyers walk through the cases, the complicating security research, and the policy options.

Speakers: Andreas Kaltsounis, Jacob Wall

SpeakerBio: Andreas Kaltsounis, BakerHostetler

Andreas Kaltsounis is an attorney and co-lead of BakerHostetler's Digital Risk Advisory & Cybersecurity practice, where he advises clients on privacy and security compliance, incident response, and regulatory defense. He holds the CISSP certification, is an IAPP Fellow of Information Privacy, and is ranked by Chambers USA and Chambers Global for his work in privacy and cybersecurity law. Before practicing law, Andreas was a managing director at an international information security consulting firm and served as a federal agent investigating criminal and national security cyber matters.

SpeakerBio: Jacob Wall, BakerHostetler

Jacob Wall is an attorney and associate in BakerHostetler's Digital Risk Advisory & Cybersecurity practice. Jacob's work spans technology regulatory law, including compliance and product counseling, regulatory defense, and policy advocacy. A particular focus of Jacob's practice is bringing a technical background to complex cybersecurity and AI regulatory questions. He and Andreas work together on a range of AI governance and cybersecurity compliance engagements for technology and critical infrastructure clients.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Whose PR Is It Anyway?

Tags: Nix Vegas Community | Creator Event/Activity

When: Saturday, Aug 8, 13:00 - 13:45 PDT

Where: LVCCW Level 1 Hall 4 1310 (Nix Vegas Community) - [Map](#)

Description:

In this audience participation-heavy session, you can get your PRs to nixpkgs reviewed and maybe even merged... if the build on one of our systems passes. Come with PRs in hand and call them out, and we'll review, build, and maybe even merge them on stage.

This is Whose PR Is It Anyway, where the version bumps are made up and the builds don't matter.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Nix Vegas Community - Friday - 13:00-13:45 PDT

Title: Whose PR Is It Anyway?

Tags: Nix Vegas Community | Creator Event/Activity

When: Friday, Aug 7, 13:00 - 13:45 PDT

Where: LVCCW Level 1 Hall 4 1310 (Nix Vegas Community) - [Map](#)

Description:

In this audience participation-heavy session, you can get your PRs to nixpkgs reviewed and maybe even merged... if the build on one of our systems passes. Come with PRs in hand and call them out, and we'll review, build, and maybe even merge them on stage.

This is Whose PR Is It Anyway, where the version bumps are made up and the builds don't matter.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Whose Resource Is It Anyway? The Design Flaw That Breaks the IAM Permission Model

Tags: Cloud Village | Creator Talk/Panel

When: Saturday, Aug 8, 12:00 - 12:20 PDT

Where: LVCCW Level 3 W313 (Cloud Village Talks) - [Map](#)

Description:

The major cloud provider's permission model is simple: use IAM to keep the bad guys out of your cloud environment. But what if the bad guys could lure victims in? Each provider implements IAM differently, and in this talk, we will explore a hidden quirk in the GCP identity boundary that allows attackers to invert the permission model and force victims into a malicious environment.

We will examine the unique aspects of GCP IAM and explore how a core design choice enabled cross-tenant account takeover via a novel vulnerability I discovered in Vertex AI Workbench, potentially leading to full cloud compromise.

The biggest threat to your cloud environment could be a project you didn't even know you were a part of.

SpeakerBio: Moshe Berntsein

Moshe Bernstein is a Senior Security Researcher specializing in cloud vulnerability research at Tenable. With over a decade of experience in cybersecurity, Moshe has developed a strong focus on network and operational security, web vulnerability research, and cloud infrastructure security. He enjoys presenting his research at conferences around the world, and is always on the lookout for new challenges.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Whose Slide Is It Anyway?

Tags: Event | Whose Slide Is It Anyway?

When: Friday, Aug 7, 22:00 - 23:59 PDT

Where: LVCCW Level 1 Hall 1 100 (Contest Stage) - [Map](#)

Description:

DEF CON 34 marks an entire DECADE of “Whose Slide Is It Anyway?” being the unholy union of improv comedy, hacking, and slide deck sado-masochism. We are the embodiment of the hacker battle cry “FUCK IT, WE’LL DO IT IN PROD.”

For the last 10 years, our team of slide monkeys have created a stupid amount of short slide decks on whatever nonsense tickles our fancies. Slides are not exclusive to technology, they can and will be about anything. Contestants will take the stage and choose a random number corresponding to a specific slide deck. They will then improvise a minimum 5 minute / maximum 10 minute lightning talk, becoming instant subject matter experts on whatever topic/stream of consciousness appears on the screen.

But....why?

Because for us, the stage is hallowed ground and since stupidity can't be stopped, we decided to weaponize it. Whether you delight in the chaos of watching your fellow hackers squirm or would like to sacrifice yourself to the Contest Gods, it's a night of schadenfreude for the whole family.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Why Couldn't I See My Own Drone? Remote ID, ESP32s, and the Packet Trail to Friend or Foe

Tags: Packet Hacking Village | Creator Talk/Panel

When: Saturday, Aug 8, 16:00 - 16:59 PDT

Where: LVCCW Level 1 Hall 3 1102 (Creator Stage 6) - [Map](#)

Description:

Friend or Foe started when adding Remote ID support to an Android airspace app still failed to detect our own DJI drone. This led us into DJI Wi-Fi Beacon behavior, vendor information elements, ESP32 promiscuous capture, and conservative evidence handling using Bayesian fusion. This talk covers practical packet analysis techniques for Remote ID (BLE and Wi-Fi), hardware tradeoffs for reliable scanning, and how to avoid turning weak signals into overconfident alerts. Attendees will learn how to build honest, low-cost RF sensors and interpret packet evidence responsibly.

Speakers: Will Hatzer, Charles Grow

SpeakerBio: Will Hatzer, Founder, GameChangersAI / Team Charity Case

Will "OGThorne" Hatzer is a security engineer, adversarial researcher, and founder of GameChangersAI. He works in security engineering at OpenAI and builds open-source tools across RF, Android, embedded systems, and defensive security. A former DEF CON Car Hacking Village speaker, his work includes a bot-detection patent and Hyundai BlueLink research later referenced by CISA.

SpeakerBio: Charles Grow, Hardware Designer / RF Researcher, Team Charity Case / GameChangersAI

Charles "OhYou_" Grow is a hardware designer, RF researcher, and ham radio operator. He designed the Friend or Foe badge hardware, solving component layout, USB-C access, GPIO conflicts, and RF ground-plane challenges. His background in fox hunting, electronics, and field debugging helped turn early prototypes into a practical, wearable device.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Misc - Saturday - 13:30-14:30 PDT

Title: Why Mandatory Age Verification Keeps Us All Less Safe

Tags: Women in Security and Privacy (WISP) | Creator Talk/Panel

When: Saturday, Aug 8, 13:30 - 14:30 PDT

Where: LVCCW Level 1 Hall 3 1100 (Creator Stage 7) - [Map](#)

Description:

Speakers: Alexis Hancock, Kenyatta Thomas

SpeakerBio: Alexis Hancock, Director of Engineering at Electronic Frontier Foundation

Alexis works to keep the networks strong and encrypted by managing the Certbot project. As well as ensuring EFF open source tools for the public are well supported. She researches an intersection of issues on digital rights, encryption, and consumer technology. She believes in an open and equitable web through encouraging expansion of security by default, bridging engineers and security research, and advocating for better and stronger tech policy and standards.

SpeakerBio: Kenyatta Thomas, Social Media and Video Manager at EFF

As the Social Media and Video Manager at EFF, Kenyatta Thomas leads the creation of digital content that educates and mobilizes the public across EFF's online platforms. They come to EFF from a background in youth and reproductive justice advocacy and organizing, having previously worked with organizations such as Physicians for Reproductive Health, the National Network of Abortion Funds, Reproaction, and Advocates for Youth. Their work as a sex educator and abortion doula informs their deep commitment to community care, access to information, and tech equity. Kenyatta believes in the transformative power of digital tools to advance justice and is committed to making online spaces more inclusive, accessible, and empowering for all.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Ham Radio Village - Saturday - 13:00-13:30 PDT

Title: Why Signals Still Matter: Amateur Radio in the Age of Cell Phones

Tags: Ham Radio Village | Creator Talk/Panel

When: Saturday, Aug 8, 13:00 - 13:30 PDT

Where: LVCCW Level 3 W315 (Ham Radio Village) - [Map](#)

Description:

Topics covered:

Why ham still matters, the philosophy of ham radio, cool stuff we're doing in the hobby with a focus on digital modes, how it's the original hacking hobby.

Extended info on software defined radio, GnuRadio.

Talk about how it's basically old school analog internet, and that everything we do on the modern internet network is possible on ham radio.

We all have radios in our pockets. 5g, Bluetooth, and heck star-link up in the sky. Let's talk about why 100 year old tech is still relevant today, and why us hackers should care about ham radio when the internet is basically everywhere now.

SpeakerBio: Nate Moore

Nate Moore works in cybersecurity, holds an Extra class amateur radio license, and spends his spare time teaching, examining, and pushing signals around the ether.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

IoT Village - Sunday - 11:00-13:30 PDT

Title: Wi-Fi Self Defense & Hacker Hunting & For Beginners

Tags: IoT Village | Creator Workshop

When: Sunday, Aug 9, 11:00 - 13:30 PDT

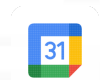
Where: LVCCW Level 1 Hall 1 215 (IoT Village) - [Map](#)

Description:

This course offers hands-on instruction using a unique, cat-shaped Wi-Fi hacking microcontroller, the Wi-Fi Nugget. Kit Cost: \$140. Class Cap: 30.

SpeakerBio: Kody Kinzie

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

IoT Village - Saturday - 12:00-13:30 PDT

Title: Wi-Fi Self Defense & Hacker Hunting & For Beginners

Tags: IoT Village | Creator Workshop

When: Saturday, Aug 8, 12:00 - 13:30 PDT

Where: LVCCW Level 1 Hall 1 215 (IoT Village) - [Map](#)

Description:

This course offers hands-on instruction using a unique, cat-shaped Wi-Fi hacking microcontroller, the Wi-Fi Nugget. Kit Cost: \$140. Class Cap: 30.

SpeakerBio: Kody Kinzie

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

IoT Village - Friday - 15:45-17:15 PDT

Title: Wi-Fi Self Defense & Hacker Hunting & For Beginners

Tags: IoT Village | Creator Workshop

When: Friday, Aug 7, 15:45 - 17:15 PDT

Where: LVCCW Level 1 Hall 1 215 (IoT Village) - [Map](#)

Description:

This course offers hands-on instruction using a unique, cat-shaped Wi-Fi hacking microcontroller, the Wi-Fi Nugget. Kit Cost: \$140. Class Cap: 30.

SpeakerBio: Kody Kinzie

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Radio Frequency Village - Friday - 17:00-17:55 PDT

Title: WiFi Shuriken: A New Architecture For High Performance Scanning

Tags: Radio Frequency Village | Creator Talk/Panel

When: Friday, Aug 7, 17:00 - 17:55 PDT

Where: LVCCW Level 1 Hall 1 409 (Radio Frequency Village) - [Map](#)

Description:

The WiFi Shuriken is a new microcontroller-based wardriving platform. The current iteration is a dual-band scanner built around a Raspberry Pi RP2350 for orchestration and six Espressif ESP32-C5 scanners. The Shuriken takes inspiration from several excellent projects in the wardriving community, but was designed around one goal: remove bottlenecks and scan as quickly and efficiently as possible.

This talk will cover how the design distributes responsibilities across the system, moves scan data, deduplicates results, tolerates failures, and leaves room for future expansion. We'll discuss why specific hardware was selected, and just as importantly, what was intentionally left out and why.

SpeakerBio: CoD_Segfault, Hard Hat Brigade

CoD_Segfault is a hardware hacker, wardriver, and retro-computing enthusiast. His projects usually center on custom electronics, embedded systems, and RF experimentation. He enjoys taking ideas from prototype to working hardware, especially when that means designing PCBs, abusing microcontrollers, or collecting wireless data in the real world. He is also part of the Hard Hat Brigade, where his builds often involve questionable ideas and putting things on his head that probably don't belong there.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Wiring the Harness: Orchestrating Frontier Models for Vulnerability Hunting at Scale

Tags: Packet Hacking Village | Creator Talk/Panel

When: Friday, Aug 7, 14:30 - 15:30 PDT

Where: LVCCW Level 1 Hall 3 1104 (Creator Stage 4) - [Map](#)

Description:

While frontier models are powerful, simply asking one to "find vulnerabilities" is far less effective than pairing with a well-designed harness, a gap that widens further down the stack and peaks at embedded firmware. During Project Glasswing, Intel scanned hundreds of repositories, from firmware to containers. This talk covers common pitfalls in LLM vulnerability hunting and presents a multi-stage harness: reconnaissance and context compression, multi-model hunting, deduplication, false positive detection, and verification. We will explore selecting the right models per stage, cutting token costs, and, the real battle, reducing false positives, especially for lower-level code where accuracy is hardest.

Speakers: Tony Martin, Arie Haenel

SpeakerBio: Tony Martin, Principal Engineer & Offensive Security Research lead at INT31 Security Research, Intel

Tony Martin is a Sr. Principal Engineer in Intel's INT31 Security Research team, where he focuses on emerging threats, software architecture and AI security. He has discovered thirty CVEs and one CWE and is senior staff at DEF CON's Packet Hacking Village.

SpeakerBio: Arie Haenel, Principal Engineer & Offensive Security Research lead, INT31 Security Research, Intel

Arie Haenel is a Principal Engineer at Intel, where he leads ASSERT, an Offensive Security Research team. He has over 25 years of professional experience, in security research and security product development on a vast number of embedded platforms, at Intel, Cisco and NDS. In his spare time, Arie teaches security engineering as an Adjunct Lecturer at the Lev Academic Center.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Witchcraft Solver: Automated 0day Discovery in Stripped Binaries

Tags: DEF CON Official Talk | Demo | Tool | Exploit

When: Sunday, Aug 9, 13:30 - 14:30 PDT

Where: LVCCW Level 1 Hall 3 904 (Main Track 4) - [Map](#)

Description:

You have a stripped binary. No source. No symbols. No harness. You want a PoC. How do you get there? Witchcraft Solver (wsolver) is a fully automated binary-only 0day discovery pipeline.

Phase 1 lifts the binary to LLVM IR via wunstrip (.eh_frame symbol recovery, 99.98% accuracy), runs an SSA taint pre-filter to cut targets by ~50%, then drives four parallel formal verification engines (KLEE, IKOS, SeaHorn, SMACK) to produce concrete violation witnesses - covering the entire binary in ~30 minutes, no source required.

Phase 2 uses those witnesses to seed directed fuzzing (AFLGo) and binary-only concolic execution (SymQEMU), converting symbolic candidates into working PoCs. An optional Phase 0 handles non-Intel targets via a lifter portfolio (RetDec + Anvill + rev.ng), covering 93% of 39,364 production ELF binaries across ARM64, ARMv7, RISC-V, and s390x.

Validated against CVE-2023-2804 (libjpeg-turbo heap-buffer-overflow): SymQEMU produces the first crash in 25 minutes from a stripped binary with zero source access.

The tool will be released under MIT license at the conference at: <https://github.com/endrazine/wsolver>

Experimental validation against the wider internet is left as an exercise to the audience...

[1] Brossard, J. "Unstripping Cloud Container ELF binaries." IEEE IC_ETC 2025. <https://ieeexplore.ieee.org/abstract/document/11141058> [2] Brossard, J. "CVE-2023-2804 Complete Fuzzing Benchmark." Zenodo. doi:10.5281/zenodo.19136269 [3] Wojtczuk, R. "UQBTng." 22C3, 2005. [4] Poeplau, S. and Francillon, A. "SymQEMU." NDSS 2021. [5] Böhme et al. "Directed Greybox Fuzzing." CCS 2017. [6] Cadar et al. "KLEE." OSDI 2008. [7] Fioraldi et al. "AFL++." USENIX WOOT 2020. [8] Brossard, J. "Introduction to the Witchcraft Compiler Collection." DEF CON 24, Las Vegas, August 2016. Video: <https://archive.org/details/youtube-1cgtr7VW7gY>

Tool Source (once published at DEF CON): <https://github.com/endrazine/wsolver>

SpeakerBio: Jonathan "endrazine" Brossard

Endrazine is a returning DEF CON speaker, having previously presented the first attack against Microsoft BitLocker and TrueCrypt in 2008, the infamous Rakshasa BIOS malware in 2012, and the Witchcraft Compiler Collection reverse engineering framework in 2016. Endrazine has previously presented at premier conferences such as Black Hat, CCC, and HITB in the industry, as well as IEEE, USENIX, and ACM in academia. He currently works as CTO at MOABI, a binary analysis and vulnerability assessment firm, after having been Principal Engineer of Product Security at Salesforce (San Francisco), where he later lead the RedTeam. He is wrapping up a PhD in reverse engineering at CNAM (Paris) where he has been an Associate Professor for three years, and holds master's degrees in Engineering, Computer Science, and Cybersecurity.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Wolfmasking: Teaching Everyday Defenders to Think Like Social Engineers

Tags: Social Engineering Community Village | Creator Talk/Panel

When: Saturday, Aug 8, 16:00 - 16:30 PDT

Where: LVCCW Level 3 W317-319 (Social Engineering Community Village) - [Map](#)

Description:

Most security awareness training keeps people in the role of prey: memorize red flags, stay vigilant, and hope your System 2 brain has enough calories left when the real attack arrives. Wolfmasking is supervised deceptive roleplay: everyday defenders safely rehearse the attacker's moves, develop a mental model of the predator, then return to defense with better instincts. This talk presents lessons and examples from a field pilot tested at Clemson University with support from CISO John Hoyt, in which roughly 80 nursing freshmen learned to construct benign social-engineering challenges, compete against one another, and report each other's attempts. The point was not to create attackers, but to create an identity shift: Students began shifting from hypothetical victims into former players: people who recognize pretext, authority, urgency, trust transfer, and emotional pressure not because they were "staying vigilant," but because they have practiced those moves themselves. I will share the four-lesson structure, guardrails, incentives, surprises, failures, and why 'practice being fooled' may matter less than 'practice doing the fooling safely.' I'll use a quick magic example to show the gap between hypothetical knowledge and lived deceptive experience. This is not a product pitch. It is a field report on a new training pedagogy for social engineering resilience.

SpeakerBio: Brian Brushwood

Brian Brushwood has spent 25 years teaching millions of people how deception works: first as a touring magician, then as creator/host of Scam School / Scam Nation, host of National Geographic's Hacking the System, creator of The Modern Rogue, and host of World's Greatest Con. His work focuses on scams, magic, persuasion, social engineering, and the mechanics of trust: how it is built, exploited, defended, and rehearsed. Through Scam School and Scam Nation, Brian spent nearly two decades turning ordinary non-deceivers into capable ethical deceivers, helping them understand cons and persuasion from the inside. Brian has delivered keynotes to audiences of thousands and recently developed an experimental offense-to-defense social engineering curriculum, piloted at Clemson University with CISO John Hoyt.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Queercon Community - Friday - 14:00-14:59 PDT

Title: Women Loving Women Meetup

Tags: Queercon Community | Creator Event/Activity

When: Friday, Aug 7, 14:00 - 14:59 PDT

Where: LVCCW Level 3 W325 (QueerCon Lounge) - [Map](#)

Description:



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Social Gatherings/Events - Friday - 20:00-23:30 PDT

Title: Women, gender non-conforming and non-binary meetup with The Diana Initiative

Tags: Meetup | The Diana Initiative

When: Friday, Aug 7, 20:00 - 23:30 PDT

Where: LVCCW Level 2 W208-209 (Diana Initiative) - [Map](#)

Description:

We'd love to get all the gender non conforming, non-binary and women together to hang out and make friends! DEF CON is better with friends. Stop in for a bit, or the whole time.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

CodeBloom - Saturday - 17:00-17:59 PDT

Title: Work Session: Binary Code

Tags: CodeBloom | Creator Workshop

When: Saturday, Aug 8, 17:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 4 1304 (CodeBloom Community) - [Map](#)

Description:

Did you know that every photo, song, and message on your phone is really just a long string of 0s and 1s? Come learn how binary code works and then turn your very own secret word into a wearable friendship bracelet using our binary alphabet chart! This session is beginner friendly and a great way to see how computers really think. If you've ever wanted to get involved in our community or teach our classes, this would be a great time to stop by and learn more!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Work Session: Binary Code

Tags: CodeBloom | Creator Workshop

When: Friday, Aug 7, 17:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 4 1304 (CodeBloom Community) - [Map](#)

Description:

Did you know that every photo, song, and message on your phone is really just a long string of 0s and 1s? Come learn how binary code works and then turn your very own secret word into a wearable friendship bracelet using our binary alphabet chart! This session is beginner friendly and a great way to see how computers really think. If you've ever wanted to get involved in our community or teach our classes, this would be a great time to stop by and learn more!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Work Session: Ciphers

Tags: CodeBloom | Creator Workshop

When: Friday, Aug 7, 14:00 - 14:59 PDT

Where: LVCCW Level 1 Hall 4 1304 (CodeBloom Community) - [Map](#)

Description:

Ever wanted to send a secret message that only your friend could read? Come build your very own cipher wheel and learn how to do exactly that! We'll walk you through the Caesar Cipher, a code used by a Roman emperor over 2,000 years ago, and show you how to pick a secret key, encrypt a message, and pass it to a friend to decrypt. This is a great hands on introduction to cryptography for folks of any age or background. If you've ever wanted to get involved in our community or teach our classes, this would be a great time to stop by and learn more!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Work Session: Ciphers

Tags: CodeBloom | Creator Workshop

When: Saturday, Aug 8, 11:00 - 11:59 PDT

Where: LVCCW Level 1 Hall 4 1304 (CodeBloom Community) - [Map](#)

Description:

Ever wanted to send a secret message that only your friend could read? Come build your very own cipher wheel and learn how to do exactly that! We'll walk you through the Caesar Cipher, a code used by a Roman emperor over 2,000 years ago, and show you how to pick a secret key, encrypt a message, and pass it to a friend to decrypt. This is a great hands on introduction to cryptography for folks of any age or background. If you've ever wanted to get involved in our community or teach our classes, this would be a great time to stop by and learn more!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Work Session: Ciphers

Tags: CodeBloom | Creator Workshop

When: Friday, Aug 7, 11:00 - 11:59 PDT

Where: LVCCW Level 1 Hall 4 1304 (CodeBloom Community) - [Map](#)

Description:

Ever wanted to send a secret message that only your friend could read? Come build your very own cipher wheel and learn how to do exactly that! We'll walk you through the Caesar Cipher, a code used by a Roman emperor over 2,000 years ago, and show you how to pick a secret key, encrypt a message, and pass it to a friend to decrypt. This is a great hands on introduction to cryptography for folks of any age or background. If you've ever wanted to get involved in our community or teach our classes, this would be a great time to stop by and learn more!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Work Session: Ciphers

Tags: CodeBloom | Creator Workshop

When: Sunday, Aug 9, 14:00 - 14:59 PDT

Where: LVCCW Level 1 Hall 4 1304 (CodeBloom Community) - [Map](#)

Description:

Ever wanted to send a secret message that only your friend could read? Come build your very own cipher wheel and learn how to do exactly that! We'll walk you through the Caesar Cipher, a code used by a Roman emperor over 2,000 years ago, and show you how to pick a secret key, encrypt a message, and pass it to a friend to decrypt. This is a great hands on introduction to cryptography for folks of any age or background. If you've ever wanted to get involved in our community or teach our classes, this would be a great time to stop by and learn more!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Work Session: Ciphers

Tags: CodeBloom | Creator Workshop

When: Saturday, Aug 8, 14:00 - 14:59 PDT

Where: LVCCW Level 1 Hall 4 1304 (CodeBloom Community) - [Map](#)

Description:

Ever wanted to send a secret message that only your friend could read? Come build your very own cipher wheel and learn how to do exactly that! We'll walk you through the Caesar Cipher, a code used by a Roman emperor over 2,000 years ago, and show you how to pick a secret key, encrypt a message, and pass it to a friend to decrypt. This is a great hands on introduction to cryptography for folks of any age or background. If you've ever wanted to get involved in our community or teach our classes, this would be a great time to stop by and learn more!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Work Session: Ciphers

Tags: CodeBloom | Creator Workshop

When: Sunday, Aug 9, 11:00 - 11:59 PDT

Where: LVCCW Level 1 Hall 4 1304 (CodeBloom Community) - [Map](#)

Description:

Ever wanted to send a secret message that only your friend could read? Come build your very own cipher wheel and learn how to do exactly that! We'll walk you through the Caesar Cipher, a code used by a Roman emperor over 2,000 years ago, and show you how to pick a secret key, encrypt a message, and pass it to a friend to decrypt. This is a great hands on introduction to cryptography for folks of any age or background. If you've ever wanted to get involved in our community or teach our classes, this would be a great time to stop by and learn more!



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Workshop Before the SIEM Blinks: How AI Memory Turns Alerts into Intelligence

Tags: La Villa Community | Creator Workshop

When: Saturday, Aug 8, 10:30 - 12:59 PDT

Where: LVCCW Level 1 Hall 4 1416 (La Villa Community) Workshops/Chillout - [Map](#)

Description:

La mayoría de los SOC's son reactivos por diseño: los eventos llegan, se almacenan, se correlacionan horas después, y en el mejor de los casos un analista los revisa cuando puede.

Este workshop rompe ese modelo.

Presentamos una arquitectura SOC-less impulsada por IA donde la detección ocurre en línea — antes de que los datos lleguen al SIEM — usando reglas Sigma traducidas a lógica ejecutable en Groovy.

Cuando una regla hace match, el evento se enriquece al instante con contexto de usuario, criticidad del activo, estructura de procesos y técnicas asociadas a MITRE ATT&CK.

El diferenciado de nuestra propuesta es la memoria. Cada alerta, ticket, resolución, triaje de analista y falso positivo alimenta un índice recurrente.

los agentes consultan ese historial para determinar si una detección es nueva, recurrente, vinculada a un activo crítico o parte de un patrón conocido — luego generan el ticket, sugieren severidad, recomiendan la contención y, en escenarios controlados la ejecutan.

El resultado del flujo es la detección y respuesta inicial medidas en segundos, no en turnos de analistas.

Speakers:Luis Pazmino,Yoshihito Adachi

SpeakerBio: Luis Pazmino, Cyber Defense Manager Banco Pichincha, Principal Consultor DataProtect Information Security

Cybersecurity Lover, Red Teamer, OSCE | OSEP | OSCP | CISM | ECSA | CEI

SpeakerBio: Yoshihito Adachi, Cybersecurity Specialist

I have a strong passion for data exploration and threat hunting, which drives me to constantly seek out new methods to detect high-level threats. Being a highly logical individual, I am deeply interested in understanding how things work. This curiosity fuels my dedication to uncovering innovative approaches and enhancing cybersecurity measures.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Wrestling with a Python: Escaping Copilot Studio's AI-Guarded Sandbox

Tags: DEF CON Official Talk | Demo | Tool | Exploit

When: Saturday, Aug 8, 15:30 - 16:30 PDT

Where: LVCCW Level 1 Hall 3 904 (Main Track 4) - [Map](#)

Description:

Microsoft Copilot Studio lets anyone build AI agents that execute Python. Behind the scenes, that code runs in a Windows container on Azure Service Fabric, wrapped in a Python sandbox and guarded by a GPT-4.1 mini model that decides what's safe to run. Three layers of defense. The presenter broke all of them.

Starting from a standard agent with code interpreter enabled, we used classic MRO introspection with string concatenation to bypass dunder filters, escaped Python entirely through pythonnet (which nobody thought to block), and systematically defeated the LLM guardrail by exploiting its leaked reasoning chain. The result: exfiltrated TLS private keys and certificates, 75 environment variables including Azure AD client IDs and Service Fabric cluster topology, complete application source code, and confirmed command execution as ContainerUser.

The most interesting finding was the LLM guardrail itself. It is non-deterministic: identical payloads sometimes pass and sometimes get blocked. It leaks its full security reasoning in the API response, turning the defender's AI into an oracle for the attacker. This talk walks through the full attack chain, demos a C2 tool that turns the code interpreter into a persistent shell, and releases all tooling.

- Ned Batchelder, "Eval really is dangerous" (2012). Original documentation of Python MRO introspection for sandbox escape.
- Michael Bargury / Zenity, "Living off Microsoft Copilot" (DEFCON 32, Black Hat USA 2024). Prompt injection and data exfiltration through Copilot connectors. Different attack surface from code interpreter sandbox escape.
- Tobias Diehl, "Mind the Data Voids: Hijacking Copilot Trust to Deliver C2 Instructions" (DEFCON 33). Memory-persistent data exfiltration via M365 Copilot. Related but targets a different feature and attack path.

Speakers: Ryan Hausknecht, Simon Maxwell-Stewart

SpeakerBio: Ryan Hausknecht, BeyondTrust

Ryan Hausknecht is the Director of Research at BeyondTrust Phantom Labs. Ryan has an extensive background in red teaming, detection development, and security research through his tenure at Microsoft and Specterops. His most notable contributions have been in cloud security as the creator of PowerZure, the Azure Threat Research Matrix, and as the co-author of AzureHound.

SpeakerBio: Simon Maxwell-Stewart, BeyondTrust

Simon Maxwell-Stewart is a Staff Security Researcher at BeyondTrust's Phantom Labs, where he focuses on cloud platform security and the emerging attack surface of enterprise AI systems. Before getting into security he spent over a decade doing data science and machine learning, with a physics degree from Oxford and production ML work in healthcare.

These days he's the resident graph nerd on the Phantom Labs team, applying graph analysis to identity security problems across Microsoft cloud environments. His recent research focuses on Entra ID attack paths, Azure infrastructure security.



Bug Bounty Village - Friday - 12:00-12:30 PDT

Title: Write Once, Shell Everywhere: Turning Arbitrary File Writes into RCE

Tags: Bug Bounty Village | Creator Talk/Panel

When: Friday, Aug 7, 12:00 - 12:30 PDT

Where: LVCCW Level 1 Hall 3 1102 (Creator Stage 6) - [Map](#)

Description:

Arbitrary file write bugs are often treated as “almost critical” findings: interesting, dangerous, but most times it’s hard to prove impact when the target does not let you write a web shell to an obvious location or overwrite some magic configuration file to achieve code execution. This talk is about closing that gap for black box approaches.

Instead of focusing on a single framework, we will present novel primitives that will make you able to pop shells across the most popular programming languages and frameworks in different ecosystems, all with as little information as possible about the target application.

The session will start by assessing the current state of the art of arbitrary file write in bug bounty style scenarios. This will set the stage for the rest of the talk as we will start building a methodology to correctly identify exploitation capabilities and obtain as much information as possible about the target.

From there, we will move into showcasing new techniques to abuse file write primitives and achieve the ultimate goal of code execution. We will go over novel techniques that apply both to the most popular interpreted languages and to the most used runtime environments.

Bug Bounty Hunters who join this talk will not only leave with fresh techniques to apply in their engagements, but with a reusable mental model for identifying their target’s execution context and proving maximum impact when faced with arbitrary file write scenarios.

Speakers: Bruno Mendes, Rafael Castilho Silva

SpeakerBio: Bruno Mendes, Head of Hacking, Ethack

Bruno Mendes is the Head of Hacking at Ethack. He began his work career as an Offensive Security Researcher on Intel's IPAS Cloud Security team in 2024. In bug bounty, back in 2023 placed 5th overall in the teams category and won the "Not Dead Yet" award at an Intigriti Live Hacking Event in Lisbon, and most recently co-authored a critical RCE with André Baptista (0xacb) that earned over \$100k+ in a single program. He has an extensive CTF background being a three-time winner of the Cybersecurity Challenge Portugal (2021-2023), captain of Team Portugal at the European Cybersecurity Challenge (2022, 2023, 2025), and won the 2023 International Cybersecurity Challenge with Team Europe. He also captained the Instituto Superior Técnico CTF team (STT) from 2022 to 2024.

SpeakerBio: Rafael Castilho Silva, Ethack

Security Researcher at Ethack focused on Vulnerability Research

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Red Team Village - Saturday - 16:00-17:59 PDT

Title: Writing Production-Grade Exploits in go-exploit

Tags: Red Team Village | Misc

When: Saturday, Aug 8, 16:00 - 17:59 PDT

Where: LVCCW Level 1 Hall 1 309 (Red Team Village) Tactic Table 4 - [Map](#)

Description:

Writing an exploit that works once in a lab is easy. Writing one that holds up across firmware versions, hardened configurations, and real-world constraints is another challenge entirely. This hands-on workshop walks through the go-exploit framework and the engineering behind real-world offensive tooling, covering go-exploit's module design, error handling, target fingerprinting, and repeatability. Attendees will leave with a working exploit and the blueprints to build more.

SpeakerBio: Landon Rice

WIP

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Writing to Shadow Stacks

Tags: DEF CON Official Talk | Demo | Exploit

When: Saturday, Aug 8, 12:30 - 13:30 PDT

Where: LVCCW Level 1 Hall 3 1007 (Main Track 2) - [Map](#)

Description:

CET shadow stacks are supposed to make return-address corruption a dead end. This talk presents three techniques that write attacker-chosen values directly into shadow stack memory on Linux.

The first uses `/proc/self/mem`. The kernel's `FOLL_FORCE` flag overrides shadow stack page protections, letting an unprivileged process write to its own shadow stack with `open()` and `pwrite()`. Works on x86-64 CET and ARM64 GCS. After our report, Linus Torvalds merged commit `599bbba5a36f` to restrict this path. A `fork+ptrace` variant still works on patched kernels. No distribution ships the new default yet.

The second uses `userfaultfd`. We register a fault handler on the shadow stack VMA, discard a page with `MADV_DONTNEED`, and when `RET` faults on the missing page, provide a replacement filled with chosen return addresses. The kernel maps it with valid shadow stack PTE encoding. Not blocked by the `/proc/self/mem` patch.

The third uses Intel's `WRSSQ` instruction, which writes to shadow stack pages from user mode. We corrected a widespread encoding bug in prior PoC code (`0x66` prefix produces `ADCX`, not `WRSSQ`) and confirmed it on Sapphire Rapids bare metal.

Validated against three CVEs (`dnsmasq`, `libinput`, `rsync`) with demos on bare metal, including a root shell with CET still enabled.

1. Intel, "Control-flow Enforcement Technology Specification," Rev. 3.0, 2019.

1. ARM, "Guarded Control Stack (GCS) Extension," Arm Architecture Reference Manual for A-profile architecture.
2. Linux kernel source, `mm/gup.c` and `fs/proc/base.c`, including `FOLL_FORCE`, `/proc/*/mem`, and `VM_SHADOW_STACK` handling.
3. Lindenmeier and Schwarz, "Ghost in the Stack: CET Shadow Stack Bypass," Black Hat Europe 2025.
4. Muench et al., "Control Flow-Oriented Programming," USENIX Security 2025.
5. Schuster et al., "Counterfeit Object-oriented Programming: On the Difficulty of Preventing Code Reuse Attacks in C++ Applications," IEEE S&P 2015.
6. CVE-2017-14493, `dnsmasq` stack buffer overflow.
7. CVE-2022-1215, `libinput` format string vulnerability.
8. CVE-2024-12084, `rsync` heap buffer overflow.

SpeakerBio: Vladimir "G1ND1L4" Tokarev, Cyera

Vladimir Tokarev is a vulnerability researcher tech lead at Cyera, specializing in Cloud, IoT/OT, Windows, Linux, and AI vulnerability research and exploit. Talks: Black Hat USA 2024 and 2023, DEF CON 33 Recon Village 2025, CodeBlue 2025, RSA 2024.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: X-Ray Your Agents: Pentesting MCPs, Skills, and the Plugin Supply Chain

Tags: AI | DEF CON Demo Labs | Intermediate | AppSec | Offense/Red Team | Purple Team | DEF CON Demo Labs

When: Saturday, Aug 8, 11:00 - 11:45 PDT

Where: LVCCW Level 1 Hall 3 900 (Demo Labs Track 4) - [Map](#)

Description:

Agents now run with thousands of third-party plugins — MCP servers, Claude skills, GPT actions, IDE extensions, plugin marketplaces — and the prevailing trust model is roughly “read the README and hope.” Tool descriptions are executable prompts. Tool parameters are executable code paths. Tool outputs feed straight into the next agent step. Yet there is no npm audit for this ecosystem, no signed manifests, and no capability sandbox in the wild.

MCP X-Ray is an open-source security scanner that ports classical pentest tradecraft to the agent plugin supply chain. It combines static config and repo audit, rules-based and LLM-driven semantic analysis, and active pentesting that actually invokes tools with adversarial inputs — emitting SARIF that drops into GitHub, VS Code, and CI gates today. In this 30-minute session we will (1) walk the threat model that ties MCPs, skills, and plugin bundles together; (2) live-demo X-Ray finding real vulnerabilities in each. Attendees walk away with a CI template they can drop in on Monday, and three intentionally vulnerable plugins to keep practicing on.

Speakers: Xia Hua, Abhijeet Kumar

SpeakerBio: Xia Hua

Xia is co-founder and CEO of Traceforce which secures AI native apps running on devices. She previously led engineering at Clumio (acquired by Commvault), delivering cloud data protection products that were 20x faster and 10x more scalable than competitors. Earlier, she was an in-memory database architect at Oracle. Xia earned her PhD in Applied Mathematics from MIT.

SpeakerBio: Abhijeet Kumar

Abhijeet Kumar is an OSCP-certified offensive security researcher and M.Eng Cybersecurity student at the University of Maryland. He has disclosed critical vulnerabilities across NASA, SAIL critical infrastructure, Keurig Dr Pepper, and U.S. government programs which includes a CVSS 10.0 RCE that triggered an official CERT-In incident response and a full account takeover chain affecting users across 20+ countries. He captains UMD's CTF team RandomHackers, which placed 1st out of 64 universities at HTB Hack The Madness 2026, and has spoken at the Billington State and Local Cybersecurity Summit alongside the Director of Adversary Emulation.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: X-Ray Your Agents: Pentesting MCPs, Skills, and the Plugin Supply Chain

Tags: AI | DEF CON Demo Labs | Intermediate | AppSec | Offense/Red Team | Purple Team | DEF CON Demo Labs

When: Friday, Aug 7, 10:00 - 10:45 PDT

Where: LVCCW Level 1 Hall 3 900 (Demo Labs Track 4) - [Map](#)

Description:

Agents now run with thousands of third-party plugins — MCP servers, Claude skills, GPT actions, IDE extensions, plugin marketplaces — and the prevailing trust model is roughly “read the README and hope.” Tool descriptions are executable prompts. Tool parameters are executable code paths. Tool outputs feed straight into the next agent step. Yet there is no npm audit for this ecosystem, no signed manifests, and no capability sandbox in the wild.

MCP X-Ray is an open-source security scanner that ports classical pentest tradecraft to the agent plugin supply chain. It combines static config and repo audit, rules-based and LLM-driven semantic analysis, and active pentesting that actually invokes tools with adversarial inputs — emitting SARIF that drops into GitHub, VS Code, and CI gates today. In this 30-minute session we will (1) walk the threat model that ties MCPs, skills, and plugin bundles together; (2) live-demo X-Ray finding real vulnerabilities in each. Attendees walk away with a CI template they can drop in on Monday, and three intentionally vulnerable plugins to keep practicing on.

Speakers: Xia Hua, Abhijeet Kumar

SpeakerBio: Xia Hua

Xia is co-founder and CEO of Traceforce which secures AI native apps running on devices. She previously led engineering at Clumio (acquired by Commvault), delivering cloud data protection products that were 20x faster and 10x more scalable than competitors. Earlier, she was an in-memory database architect at Oracle. Xia earned her PhD in Applied Mathematics from MIT.

SpeakerBio: Abhijeet Kumar

Abhijeet Kumar is an OSCP-certified offensive security researcher and M.Eng Cybersecurity student at the University of Maryland. He has disclosed critical vulnerabilities across NASA, SAIL critical infrastructure, Keurig Dr Pepper, and U.S. government programs which includes a CVSS 10.0 RCE that triggered an official CERT-In incident response and a full account takeover chain affecting users across 20+ countries. He captains UMD's CTF team RandomHackers, which placed 1st out of 64 universities at HTB Hack The Madness 2026, and has spoken at the Billington State and Local Cybersecurity Summit alongside the Director of Adversary Emulation.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: xEndity: IoT Firmware Analysis & Digital Twin Platform

Tags: DEF CON Demo Labs | Intermediate | Defense/Blue Team | Hardware/IoT | Offense/Red Team | Purple Team | Threat Intel/Hunting | DEF CON Demo Labs

When: Saturday, Aug 8, 16:00 - 16:45 PDT

Where: LVCCW Level 1 Hall 3 1001 (Demo Labs Track 1) - [Map](#)

Description:

IoT devices are embedded in critical infrastructure globally, yet security teams face a fundamental constraint: you cannot aggressively test what you cannot safely replicate. Physical hardware is expensive, limited in supply, and testing against production systems is off-limits. This leaves defenders operating blind against an expanding attack surface of billions of connected devices.

xEndity is an open-source, end-to-end IoT firmware emulation platform that transforms raw firmware binaries into fully functional, network-ready virtual device instances, no physical hardware required. It provides an automated pipeline spanning firmware acquisition, binary analysis, filesystem extraction, emulation packaging, and orchestrated deployment of emulated device networks at scale.

The platform enables two high-impact use cases: first, as a scopeless penetration testing range where red teams and researchers can conduct unrestricted vulnerability validation, exploit development, and attack simulation against realistic IoT environments. Second, as a deceptive defense layer where emulated devices are deployed as high-interaction honeypots to capture adversary tradecraft, collect OS-level and network telemetry, and generate actionable threat intelligence.

Speakers: Zeus "LightningGod" Chan, Kenneth "kenleejl" Lee

SpeakerBio: Zeus "LightningGod" Chan

Zeus Chan is a security researcher on the Adversary Emulation Team at HTX (Home Team Science and Technology Agency), where he focuses on IoT firmware analysis, device emulation, and offensive security research. His work spans building automated pipelines for firmware emulation, security testbed development, and honeypot deployment for threat intelligence collection against embedded systems. Zeus has presented IoT security research at DEFCON events globally and Milipol TechX Singapore, and has supported community initiatives including the HTX Public Safety Village at DEFCON Singapore. He holds experience in red team operations supporting critical national infrastructure across the finance and healthcare sectors.

SpeakerBio: Kenneth "kenleejl" Lee

Cyber security enjoyer

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: xEndity: IoT Firmware Analysis & Digital Twin Platform

Tags: DEF CON Demo Labs | Intermediate | Defense/Blue Team | Hardware/IoT | Offense/Red Team | Purple Team | Threat Intel/Hunting | DEF CON Demo Labs

When: Friday, Aug 7, 13:00 - 13:45 PDT

Where: LVCCW Level 1 Hall 3 1001 (Demo Labs Track 1) - [Map](#)

Description:

IoT devices are embedded in critical infrastructure globally, yet security teams face a fundamental constraint: you cannot aggressively test what you cannot safely replicate. Physical hardware is expensive, limited in supply, and testing against production systems is off-limits. This leaves defenders operating blind against an expanding attack surface of billions of connected devices.

xEndity is an open-source, end-to-end IoT firmware emulation platform that transforms raw firmware binaries into fully functional, network-ready virtual device instances, no physical hardware required. It provides an automated pipeline spanning firmware acquisition, binary analysis, filesystem extraction, emulation packaging, and orchestrated deployment of emulated device networks at scale.

The platform enables two high-impact use cases: first, as a scopeless penetration testing range where red teams and researchers can conduct unrestricted vulnerability validation, exploit development, and attack simulation against realistic IoT environments. Second, as a deceptive defense layer where emulated devices are deployed as high-interaction honeypots to capture adversary tradecraft, collect OS-level and network telemetry, and generate actionable threat intelligence.

Speakers: Zeus "LightningGod" Chan, Kenneth "kenleejl" Lee

SpeakerBio: Zeus "LightningGod" Chan

Zeus Chan is a security researcher on the Adversary Emulation Team at HTX (Home Team Science and Technology Agency), where he focuses on IoT firmware analysis, device emulation, and offensive security research. His work spans building automated pipelines for firmware emulation, security testbed development, and honeypot deployment for threat intelligence collection against embedded systems. Zeus has presented IoT security research at DEFCON events globally and Milipol TechX Singapore, and has supported community initiatives including the HTX Public Safety Village at DEFCON Singapore. He holds experience in red team operations supporting critical national infrastructure across the finance and healthcare sectors.

SpeakerBio: Kenneth "kenleejl" Lee

Cyber security enjoyer

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Yes, I froze an SNES for science

Tags: Game Hacking Village | Creator Talk/Panel

When: Sunday, Aug 9, 11:30 - 12:30 PDT

Where: LVCCW Level 1 Hall 3 801 (Creator Stage 2) - [Map](#)

Description:

"dwangoAC describes why he put a SNES console in a freezer, the scientific process that led to unexpected statistics, and whether or not it helped TASBot play Super Metroid Tool-Assisted Speedruns on real consoles. This talk will cover how 1990's-era component aging affects RNG and why hotplate% speedruns don't work the way the speedrunning community thinks they do

SpeakerBio: dwangoAC

dwangoAC is the keeper of TASBot, a cute non-AI robot. TASBot presses buttons perfectly like a player piano and plays games fast, often employing game breaking glitches. TASBot content has helped raise more than \$1.5M at Games Done Quick and other charity events since 2013. dwangoAC is known for video game science experiments, investigations, and transformative art.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Radio Frequency Village - Saturday - 16:00-16:25 PDT

Title: Yes, it runs Doom: over the air gaming on a bladeRF SDR

Tags: Radio Frequency Village | Creator Talk/Panel

When: Saturday, Aug 8, 16:00 - 16:25 PDT

Where: LVCCW Level 1 Hall 1 409 (Radio Frequency Village) - [Map](#)

Description:

This presentation will demo and discuss the development of a Doom port running on the Nuand BladeRF 2.0 micro xA9 Software Defined Radio.

The BladeRF is designed for RF development, containing a Cyclone V FPGA and a radio frontend capable of up to 6GHz, but lacks a hard CPU and general-purpose memory, making it a strange and particularly entertaining candidate for a game port.

This project combines FPGA design, customized firmware, RF-based video transmission, and wireless controller support. The talk will walk through system architecture, including the game engine port, how video signal is generated and transmitted, and how wireless controller input is handled. It will also cover the challenges, compromises, and unexpected findings that shaped the final design.

SpeakerBio: max

Max is an enthusiast of strange hardware, with particular interests in retro computing and game development. He's spent years restoring vintage game consoles and computers, experimenting with VR tracking interfaces, and building hardware projects to combine these interests. Professionally, Max designs custom hardware for RF collection and security systems.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Yet Another Walking Dead of Active Directory

Tags: Adversary Village | Creator Talk/Panel

When: Friday, Aug 7, 12:00 - 12:30 PDT

Where: LVCCW Level 1 Hall 3 1105 (Creator Stage 3) - [Map](#)

Description:

Disabled Active Directory accounts are commonly treated as harmless remnants of the past. In reality, many of these “dead” objects still retain dangerous inbound permissions, historical privilege artifacts, inherited ACL relationships, and hidden attack paths that most organizations never investigate.

This talk demonstrates how disabled users, computers, and service accounts can still become active participants in privilege escalation chains through misconfigured DACLS, AdminSDHolder side effects, nested group inheritance, and delegated permissions. Through a real-world inspired case study, attendees will learn how a seemingly low-privileged user leveraged hidden rights over a disabled account to move toward Domain Admin in a mature enterprise environment.

The presentation also introduces LazarusWakeUp, a tool designed to identify and analyze disabled Active Directory principals with dangerous inbound relationships, helping operators uncover hidden privilege escalation paths involving forgotten identities that traditional enumeration techniques and BloodHound analysis may overlook.

Additionally, the talk presents a new perspective on Active Directory Recycle Bin abuse and object resurrection, showing how deleted identities may continue to create security risks even after organizations believe they have been removed entirely.

SpeakerBio: Nikos "nickvourd" Vourdas, EY

Nikos Vourdas, also known as nickvourd or NCV, is a Senior Offensive Security Consultant based in the US. With over five years of professional experience, he has actively participated in various global Tiber-EU and iCAST Red Teaming engagements. Nikos has conducted full Red Teaming operations to major clients across retail, banking, shipping, construction industries. He holds OSCE3, OSCP, OSWP, CRTL, CRT0 and OASP certifications. Also, he has previously presented at DEF CON, DevSecCon, and various BSides events around the world. Nikos loves contributing to open-source projects and always starts his day at 05:00 AM with a refreshing jog while listening to French rap music.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

The Diana Initiative - Saturday - 10:00-10:59 PDT

Title: Yoga

Tags: The Diana Initiative | Creator Event/Activity

When: Saturday, Aug 8, 10:00 - 10:59 PDT

Where: LVCCW Level 2 W209 (Diana Initiative) - [Map](#)

Description:

Come join us for morning yoga and meditation. This workshop is inclusive of all bodies. Meditation can help quiet the mind, manage stress, and enhance overall emotional well-being, making it a great way to start the day.

SpeakerBio: Deanna Heon

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

The Diana Initiative - Friday - 17:00-17:59 PDT

Title: Yoga

Tags: The Diana Initiative | Creator Event/Activity

When: Friday, Aug 7, 17:00 - 17:59 PDT

Where: LVCCW Level 2 W209 (Diana Initiative) - [Map](#)

Description:

Come join us for morning yoga and meditation. This workshop is inclusive of all bodies. Meditation can help quiet the mind, manage stress, and enhance overall emotional well-being, making it a great way to start the day.

SpeakerBio: Deanna Heon

No BIO available



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: You Can't Block My C2 — It's Your Google Calendar

Tags: Red Team Village | Misc

When: Saturday, Aug 8, 13:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 1 309 (Red Team Village) Workshop Stage 1 - [Map](#)

Description:

Speaker Bio

Nishant Tayade is a Security Engineer on an enterprise Red Team, where he has spent three years conducting internal and external red team campaigns simulating real-world adversary tactics. His current research explores covert command-and-control techniques — including Mythic agents that abuse legitimate cloud services for stealthy communication — and operationalizing AI agents to enhance offensive security operations. Prior to his current role, he spent two years in SOC and SIEM engineering, giving him a full-stack perspective on both offense and defense.

Nishant holds a Master of Science in Information Security from Carnegie Mellon University. He has spoken at BSides Seattle, BSides San Diego, and BSides New Orleans, covering topics ranging from anonymity and OPSEC to how attackers weaponize OSINT and AI to profile targets.

This research started during an APT41 emulation campaign he led, where he mapped the group's real-world tradecraft — including their use of Google Calendar as a C2 channel. While building the simulation, he observed that cloud service API traffic to domains like googleapis.com was effectively invisible to enterprise detection stacks. Most cloud-native organizations allowlist this traffic by default, creating a blind spot. He built Chronos and Epoch to operationalize that technique within Mythic, and validated that Calendar-based C2 traffic went undetected against production monitoring.

Description

What if C2 traffic was indistinguishable from a Google Calendar sync? This session presents Chronos and Epoch — a Mythic agent and C2 profile that use Google Calendar as a dead-drop communication channel. All traffic flows to googleapis.com over standard HTTPS. There is no C2 server IP for defenders to discover, no infrastructure to burn, and no way to block it without disrupting enterprise calendar workflows.

The workshop covers the journey of building a functional C2 channel over a SaaS API that was never designed for it — the architectural decisions, the operational tradeoffs, and the hard lessons learned when things broke in unexpected ways. The Calendar API has no push notifications, inconsistent event visibility across clients, and was never designed for reliable message passing. Making a reliable C2 agent on top of that required solving problems that don't exist in traditional HTTP-based C2. The engineering challenges along the way revealed lessons that apply well beyond Calendar C2.

The session will cover: - Why Google Calendar makes an effective covert channel for C2 and where it falls short - How encrypted tasking is hidden inside calendar event metadata - Using Calendar C2 as a fallback channel when primary C2 infrastructure gets burned - Low-and-slow operations: credential harvesting, recon, and maintaining access in heavily monitored environments - When to deploy this on an engagement and when HTTP-based C2 is the better choice - The defender's perspective: Calendar API audit logs, event creation/deletion frequency anomalies, extendedProperties usage patterns, and service account authentication from unexpected IPs

Both components will be open-sourced on GitHub for the community.

Workshop Breakdown (30 minutes)

Intro — 2 minutes - Who the presenter is, background - The premise: C2 traffic hiding inside legitimate Google Calendar API calls

Why Google Calendar — 5 minutes - The dead-drop C2 concept and why Calendar is uniquely suited - googleapis.com is allowlisted everywhere, event metadata is invisible in the UI - What existed before and what was missing

Architecture with pre-recorded demo — 6 minutes - Epoch: transparent relay that never decrypts payloads - Chronos: Python agent with encrypted Calendar communication - Pre-recorded demo: checkin, command execution, file browser, multi-agent

Lessons learned — 7 minutes - What broke: Calendar API visibility delays, silent task drops, racing server instances - What it taught about building C2 over SaaS APIs

Red team applications and defense — 7 minutes - Fallback channel: what to do when your HTTP C2 gets burned and you need to maintain access - Low-and-slow ops: credential harvesting, recon, and staging for re-entry - When Calendar C2 is the right tool and when it isn't - Calendar API audit logs, event pattern anomalies, detection strategies

Close — 3 minutes - Key takeaways, GitHub release, transition to tactic

Tactic Breakdown (2 hours, multiple waves)

Each wave runs approximately 30-40 minutes with 10-15 attendees:

Setup and installation — 10 minutes - Install Epoch C2 profile and Chronos agent into Mythic using mythic-cli - Verify containers are running and registered

Configuration — 10 minutes - Configure Google Calendar integration with a service account - Set calendar ID, poll interval, and credentials in the Mythic UI - Start the C2 profile

Build and deploy — 5 minutes - Build a Chronos payload through the Mythic UI - Deploy the agent on their own VM

Operate — 10 minutes - Issue commands through Mythic: shell, ls, whoami, cat, download - Observe the file browser integration - Watch calendar events appear and disappear in real time

Defender perspective — 5 minutes - Examine Google Workspace Calendar API audit logs - Identify anomalies: rapid event creation/deletion cycles, extendedProperties.private usage (legitimate apps rarely use this), service account authentication from unexpected IPs - Discuss what blue teams should monitor for and why this is detectable if you know where to look

Prerequisites: Attendees should bring their own Linux VM or cloud instance with Mythic installed. A setup guide will be provided in advance. Pre-configured Google Cloud service account credentials will be provided at the table so attendees don't need their own GCP project — they can start operating immediately.

SpeakerBio: Nishant Tayade

Nishant is a Security Engineer specializing in Adversarial Emulation, Red Teaming and OSINT. He focuses on simulating real-world threats to enhance enterprise security. Prior to that, he earned his master's degree in security from Carnegie Mellon University.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: You Can't Opt Out: The Invisible Surveillance in Your Walls, Pockets, and Lives

Tags: IoT Village | Creator Talk/Panel

When: Sunday, Aug 9, 10:00 - 10:59 PDT

Where: LVCCW Level 1 Hall 3 1105 (Creator Stage 3) - [Map](#)

Description:

Surveillance is baked into the very fabric of our digital existence. From smart homes to smart cars, and now we drive down streets with smart cameras tracking our every move. And why aren't even aware of most of it, because almost none of it is disclosed in any meaningful way to the people being surveilled. Sometimes because companies don't want their users to understand what data they're collecting, because users would be upset, and sometimes because governments do want us to know about the surveillance. This talk walks through a series of real cases where surveillance was hiding in plain sight inside ordinary consumer IoT devices and apps, and was only discovered because someone with the right skills bothered to look. From high school students at a previous DEF CON uncovering microphones installed in school bathrooms, to Byron Tau's reporting on commercial SDKs (like the one embedded in a widely-used Muslim prayer app) feeding location data to U.S. military and intelligence buyers, to robot vacuums quietly mapping the interiors of homes and shipping that data overseas, to the BadBox 2.0 botnet found lurking inside off-the-shelf Android streaming boxes like Superbox. The surveillance is pervasive, and the average consumer has no realistic way to detect or refuse it. This session makes the case that the question is no longer "are you being watched?" but "could you even opt out if you tried?" The reality is, it's becoming so difficult to have meaningful privacy in the digital age that we're on the cusp of a digital panopticon that threatens the very freedom of society. This talk explains what is at stake to democracy when privacy disappears, and how it slowly eliminates the self-correcting mechanisms and checks on power in society, such as protest movements, whistleblowers, independent media, protest movements, activist groups, and opposition parties. It is also a call to action for the people in this room, who possess the unique skill sets of reverse engineering, network analysis, firmware teardown, RF work etc. People breaking these systems apart and revealing what they find to the world is rapidly becoming the only meaningful check on a landscape that has decided surveillance is the default. We need more researchers looking, and we need them looking now.

SpeakerBio: Naomi Brockwell

No BIO available

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: You Hold the Helm: Agentic LLM Workflows for Malware Reversing

Tags: Malware Village | Creator Talk/Panel

When: Friday, Aug 7, 16:35 - 17:15 PDT

Where: LVCCW Level 1 Hall 2 600 (Malware Village) Talks - [Map](#)

Description:

Malware analysts are integrating LLMs into their reversing workflows today, in real casework. The MCP integrations for IDA Pro, Ghidra, radare2, and Binary Ninja already exist and are publicly available, and analysts are using them to rename functions, triage samples, and hunt for vulnerabilities. Adoption has outpaced any measured account of where these tools are reliable and where they are not. There is also a cost problem that gets little attention: running an agent against a single sample can burn an enormous number of tokens, much of it spent having the model rediscover the same things on every binary. This session addresses both. We built an agentic malware analysis framework, tested it across multiple models and real samples scored against ground truth, and we are bringing the numbers along with the workflows. The framework connects LLMs directly to disassemblers and decompilers through MCP, and wraps that with per-language skills for the malware families analysts actually encounter: C and C++, C#, Go, and Android. Each skill encodes what the runtime looks like, how the decompiler tends to mangle that specific target, which structures and metadata are worth recovering first, and what the model can safely ignore. The Go skill carries knowledge of the pcIntab and the runtime's calling conventions. The C# skill assumes IL and metadata tables rather than native code. The Android skill separates the DEX, the native libraries, and the manifest, and knows where behavior usually hides. The skills exist for efficiency. Without them, the model relearns the same Go runtime layout on every sample and pays the same token cost to reach the same conclusion. With them, that context is supplied once and the model spends its budget on the sample. The framework runs inside Docker containers orchestrated through an ADK agent loop. Three concrete reasons make this matter. Isolation keeps live malware analysis off the host. Reproducibility means the same container, skill, and sample produce similar starting conditions every time, which is what makes any claim about model performance meaningful. Disposability means that when an agent corrupts its own analysis state, and it will, you tear the container down and start clean rather than nursing a polluted session. The ADK loop is what lets the agent act on its own: pulling function lists, following cross-references, reading decompiled output, and issuing disassembler commands. It is also where most of the interesting failures show up when the agent is not constrained. Function renaming and summarization on stripped binaries holds up well, but only when functions are fed with surrounding call context rather than dumped in bulk. Behavioral triage, the question of what a sample does and where to look first, is faster through the agent than manual function-list review, and the benefit is largest for less experienced analysts. Pattern matching across a binary is reliable when you specify the class of issue to look for. The per-language work also pays off on Go and Rust samples, where traditional C and C++ oriented decompilers produce walls of indistinguishable functions and the LLM-assisted workflow often cuts through what the tooling alone cannot. The failures matter as much as the wins. Crypto identification is where the models are most confidently wrong, mapping anything stream-cipher-shaped onto whatever algorithm they saw most in training. Deobfuscation of any serious protection scheme breaks down quickly. CVE matching is the most consequential failure, because a fabricated CVE number reads with the same authority as a real one, and an analyst who puts it into a threat report has introduced an error that is hard to catch later and can misdirect incident response. Scope drift shows up throughout: left unconstrained, the agent will decide on its own that you wanted detection rules when you asked for unpacker analysis. We show each of these failure modes on screen with the actual model output. The core of the session is a direct comparison, the same model and the same sample, run two ways. First pass is a minimal prompt with the agent left to default behavior. Second pass, we drive, selecting which functions to examine, supplying context through the right per-language skill, and constraining the output format. The model does not get smarter between passes. We get more deliberate about how we use it, and the output diverges sharply. That is the thesis as a demo rather than a claim: the analyst is the captain and the model is the crew, and analysis quality tracks almost entirely with how well it is steered. We walk the comparison side by side on real samples, and ship the demo binaries and both prompt sets with the talk. Attendees leave learning how to do a full setup: the Docker containers, the ADK agent scaffolding, the per-language skills for C and C++, C#, Go, and Android, and the prompt templates that worked alongside the ones that did not. They can install it, run the same comparisons we ran, and extend the evaluation to their own samples and analysis tasks. They also leave with a calibrated sense of which tasks are safe to hand to an agent, which require careful steering, and which should never be trusted without manual verification. Additionally, we will open source our framework the day of the talk.

Speakers: Asher Davila, Lenin Alevski

SpeakerBio: Asher Davila, Vulnerability Researcher at Palo Alto Networks

Passionate about binary analysis, binary exploitation, reverse engineering, hardware hacking, retro computing, and music.

SpeakerBio: Lenin Alevski, Security Engineer at Google

Lenin Alevski is a Full Stack Engineer and generalist with a lot of passion for Information Security. Currently working as a Security Engineer at Google. Lenin specializes in building and maintaining Distributed Systems, Application Security and Cloud Security in general. Lenin loves to play CTFs, contributing to open-source and writing about security and privacy on his personal blog <https://www.alevsk.com>.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: You're Hired... Maybe: Inside Cybersecurity Hiring in 2026

Tags: Blue Team Village | Creator Talk/Panel

When: Sunday, Aug 9, 11:00 - 11:59 PDT

Where: LVCCW Level 2 W217 (Blue Team Village) Main Stage - [Map](#)

Description:

Speakers: George Scheibe, Neha Gautam, Sherry Michael, Siddharth Kumar

SpeakerBio: George Scheibe

George received his letterman jacket for Computer Science in high school and has been nerding out ever since. From a Multichannel Transmission Systems Operator-Maintainer in the US Army to the sole IT person for an entire resort, George has done everything from global network monitoring in command centers to toning out sea salt corroded POTS lines in crawl spaces. These days though you'll find him working in a SOC helping to develop the next generation of cyber security professionals.

SpeakerBio: Neha Gautam

Neha Gautam is a Product Manager at Microsoft Security and a Carnegie Mellon graduate specializing in the intersection of Identity and AI. From scaling platforms at Walmart to securing agentic AI at Microsoft, Neha's mission is to translate complex security hurdles into seamless product experiences. She is a passionate mentor for women in tech and a frequent volunteer for WiCyS and Defcon Blue Team Village. Neha believes that the future of computing must be built by diverse perspectives—a philosophy she champions whether she's designing enterprise governance or coaching early-career professionals.

SpeakerBio: Sherry Michael

Sherry Michael is the security technical director for Information systems and computing at the University of Pennsylvania, a prestigious Ivy League university and research institution in Philadelphia. With more than thirty years of experience in information technology and over twelve years focused on cybersecurity, Sherry brings deep expertise in securing complex enterprise environments and fostering cross team collaboration. In addition to technical leadership responsibilities, Sherry serves on hiring panels for a wide range of technical positions and acts as a hiring officer. She is passionate about identifying and developing the next generation of technology and security professionals.

SpeakerBio: Siddharth Kumar

Siddharth Kumar is the Offensive Security Lead at Ethical Intruder. He breaks into enterprise environments for a living, following attack paths through Active Directory, cloud infrastructure, web applications, and occasionally the strange world of operational technology. Previously, he led red team operations at EY and earned a master's degree in information security from Carnegie Mellon University. Siddharth is particularly interested in identity attacks, advanced Web/API exploitation, adversary tradecraft, and the small security oversights that lead to very large compromises. When he is not breaking into things professionally, he enjoys helping other security practitioners develop their technical skills and navigate careers in offensive security.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: You're Probably Using FPE Wrong

Tags: Crypto & Privacy Village | Creator Talk/Panel

When: Friday, Aug 7, 14:30 - 14:59 PDT

Where: LVCCW Level 1 Hall 3 1102 (Creator Stage 6) - [Map](#)

Description:

Format-preserving encryption is widely deployed and widely misunderstood. It appears in PCI environments, GDPR compliance architectures, banking systems, payment platforms, and legacy applications where changing the data format is not an option. Unfortunately, many production uses of FPE get the important details wrong.

This talk is a practical field guide to FPE.

We will walk through NIST FF1 and FF3-1 from the perspective of someone building or reviewing a real system. The focus is not on cryptographic theory for its own sake, but on the decisions that matter in production: choosing the radix, understanding domain-size limits, using tweaks correctly, and recognizing when the security margin is thinner than it looks. We will also talk about the key management problem that most FPE libraries leave unresolved.

Finally, we will separate good use cases from bad ones. FPE can be the right tool for structured sensitive data, legacy systems, and format-constrained workflows. It can also be the wrong tool, especially when small domains, poor key separation, missing tweaks, or assumptions borrowed from tokenization creep into the design.

SpeakerBio: Leslie Gutschow

Principal engineer and founder of Horizon Digital Engineering. Named inventor on two US patents covering format-preserving encryption and string protection techniques (OpenText/Micro Focus). Former Principal Architect and Professional Services at Micro Focus/Voltage Security (7 years) — led enterprise FPE deployments and integrations across financial services, healthcare, and retail. Previously: Naval Research Lab, Boeing. Currently researching memory-safe OS infrastructure.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: You've Got Mail (That Was Meant For No One)

Tags: DEF CON Official Talk | Tool

When: Friday, Aug 7, 17:30 - 17:59 PDT

Where: LVCCW Level 1 Hall 3 904 (Main Track 4) - [Map](#)

Description:

In 2020, I registered a domain on a whim, mostly because I thought it would be hilarious for email, and then forgot about it. Then a city government faxed me their internal documents. Then an organization started sending me Cisco UCM alerts. Then 363,000 emails arrived in sixteen months. I never sent a single packet of attack traffic. The vulnerability is an assumption, that a domain nobody owns is safe to hardcode. Developers at enterprise software vendors, government agencies, and companies made that assumption. I registered the domains and the mail flowed in. This talk covers six years of passive email interception across more than 20 domains, the tooling built to systematically map this attack surface across hundreds of TLDs, and what 400,000 misdirected emails reveal about how production mail infrastructure actually fails. No exploits. No credentials. Just a \$11 domain registration.

Sheward, M. "Deleteduser.com -- a \$15 PII Magnet." Medium, April 2026.
<https://mike-sheward.medium.com/deleteduser-com-a-15-pii-magnet-c4396eb21061>

Krebs, B. "They Told You Not To Reply." Washington Post Security Fix, March 2008.
https://web.archive.org/web/20200905092128/http://voices.washingtonpost.com/securityfix/2008/03/they_told_you_not_to_reply.h

Krebs, B. "Chipotle Serves Up Chips, Guac & HR Email." Krebs on Security, 16 Nov. 2015,
<https://krebsonsecurity.com/2015/11/chipotle-serves-up-chips-guac-hr-email/>

Fitzpatrick, J. "Sears-Kmart MyGofer," Internet Archive, archived May 1, 2014,
<https://web.archive.org/web/20140501153309/http://sears-kmart-mygofer.com/>

Kim, P. and Gee, G. "Doppelganger Domains." Godai Group, 2011.
<https://godaigroup.net/wp-content/uploads/doppelganger/Doppelganger.Domains.pdf>

Szurdi, J. and Christin, N. "Email Typosquatting." IMC 2017. ACM. <https://dl.acm.org/doi/10.1145/3131365.3131399>

Internet Assigned Numbers Authority. "RDAP Bootstrap File for Domain Name Space." <https://data.iana.org/rdap/dns.json> (RFC 7484)

Bradner, S., "RFC 2606: Reserved Top Level DNS Names", IETF, 1999 <https://www.rfc-editor.org/rfc/rfc2606>

Klensin, J., "Simple Mail Transfer Protocol", RFC 5321, IETF, October 2008. <https://www.rfc-editor.org/rfc/rfc5321>

DomainTools. "TLD Registration Count Statistics." <https://research.domaintools.com/statistics/tld-counts/>

SpeakerBio: Cøry "interpunkt" Solovewicz

Cory Solovewicz (aka interpunkt) is a security consultant specializing in web and mobile application testing. His path into security started early, experimenting with tools like Sub7 and learning how systems could be pushed beyond their intended use. After a career in full-stack development, he transitioned into security to focus on breaking and improving real-world systems. He brings a builder's perspective to his work, shaped by years of coding, late nights in hackerspaces, and a curiosity for how things fail.



Bug Bounty Village - Saturday - 10:45-11:30 PDT

Title: You're Invited to Get Hacked: Real-World Exploits in Modern Invitation Systems

Tags: Bug Bounty Village | Creator Talk/Panel

When: Saturday, Aug 8, 10:45 - 11:30 PDT

Where: LVCCW Level 2 W206-207 (Bug Bounty Village) - [Map](#)

Description:

Invitation flows are designed to maximize growth, not withstand attackers, and that makes them a goldmine for security researchers. Hidden behind trusted onboarding journeys are assumptions about identity, unchecked state transitions, and high-impact vulnerabilities that automated scanners routinely miss. In this talk, I'll walk through three real-world disclosures that led to account takeover, stealthy privacy manipulation, and permanent account lockout. You'll leave with a practical methodology for uncovering these overlooked flaws and a fresh hunting ground that many researchers still ignore. If you've been skipping invitation flows, you've been leaving money on the table.

SpeakerBio: Ali "logic-breaker" Kabeel

With over a decade of bug hunting experience, Ali has uncovered critical vulnerabilities across top tech platforms including Google, Microsoft, Meta, and Snapchat. He's especially passionate about business logic vulnerabilities, flaws rooted in real-world misuse rather than broken code, because they often evade automated scanners yet carry high impact. Ali is currently a Security and Privacy Engineering Lead at Bending Spoons, where he leads security efforts across major products including WeTransfer, Brightcove, and Vimeo. He actively shares his expertise through conference talks, mentoring, and community engagement.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Your Bank Thinks I'm You: A Complete Kill Chain Against Mobile Banking Security

Tags: DEF CON Official Talk | Demo | Tool | Exploit

When: Friday, Aug 7, 15:30 - 16:30 PDT

Where: LVCCW Level 1 Hall 3 1007 (Main Track 2) - [Map](#)

Description:

Mobile banking apps stack multiple security layers: RASP (runtime protection), root/jailbreak detection, anti-instrumentation, biometric KYC with liveness detection, and AI-powered anti-deepfake. Each layer promises to stop attackers. We defeated all of them -- in production apps used by millions.

We present a full kill chain against mobile banks and digital wallet apps from a Latin American country, demonstrating how an attacker with an Android phone and open-source tools can: (1) bypass RASP and root detection using kernel-level root solutions and publicly available modules, achieving 100% evasion of OS integrity and anti-hacking controls; (2) use Frida to dynamically instrument biometric SDKs, injecting controlled frames into the liveness capture flow by hooking the "best result" getter and replacing the YUV buffer; (3) bypass KYC identity verification by substituting selfie images and crafting coherent template+photo payloads that the backend accepts as legitimate; and (4) generate AI-synthetic faces from photos that pass liveness detection with 0% detection rate.

Every banking app we tested fell. The different RASPs and biometric SDKs are deployed in 30+ countries, protecting hundreds of millions of users. We'll show why that should worry you. Video demos included.

1. KernelSU Project - <https://kernelsu.org>
2. Kitsune Magisk Fork - <https://github.com/1q23lyc45/KitsuneMagisk/tree/kitsune>
3. Frida Dynamic Instrumentation Toolkit - <https://frida.re>
4. JADX Decompiler - <https://github.com/skylot/jadx>
5. RootBeerSample Root Detection Tool - <https://github.com/nickcaballero/RootBeerSample> (reference implementation)
6. TMLP Team / GooseBt Studio - Root bypass module configurations (GitHub, publicly available)
7. ImNotADeveloper - Xposed module that hides developer mode and USB debugging status from app detection - <https://github.com/auag0/ImNotADeveloper>
8. Public KYC bypass repositories (referenced for threat landscape awareness):
 - ◆ <https://github.com/kycbypass/Android-Phone-Bypass-KYC-verification---No-root-required>
 - ◆ <https://github.com/hxreborn/biometric-bypass>
 - ◆ <https://github.com/nocomp/deep-offensive-ai>

Speakers: Xavier "@xaferima" Riofrio Machado, Alex Tipan

SpeakerBio: Xavier "@xaferima" Riofrio Machado, Fintech Ecuador

Computer Science Engineer with an MSc in Cybersecurity, specialized in offensive security, vulnerability research, and adversarial analysis, with a strong focus on mobile (Android & iOS) security.

I identify systemic weaknesses through logical reasoning, abuse of flawed assumptions, and hands-on exploitation of complex workflows across mobile, web, and API-driven environments. My experience combines deep technical rigor with practical red teaming, allowing me to model realistic attack paths instead of theoretical risks.

I have worked in high-demand environments such as CERN and currently contribute to securing fintech and digital wallet ecosystems, where mobile platforms are critical attack surfaces. While offense-driven by design, I translate offensive findings into concrete defensive controls that actually withstand real-world attackers.

SpeakerBio: Alex Tipan, Fintech Ecuador

Cybersecurity professional specialized in application security, with a focus on offensive analysis of mobile apps, bypassing RASP controls, and assessing facial biometric workflows. Since school, he has been self-taught in programming, hacking, Linux, networking, and cryptography, later strengthening his academic foundation through a degree in Computer Systems Engineering. He currently conducts hands-on research on protection evasion in financial applications, including advanced instrumentation techniques and validation of real-world risks in authentication processes. His work aims to translate complex technical findings into concrete defensive security improvements.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Your Infrastructure Is a DAG: Manage It With Nix

Tags: Nix Vegas Community | Creator Talk/Panel

When: Saturday, Aug 8, 15:30 - 16:30 PDT

Where: LVCCW Level 1 Hall 4 1310 (Nix Vegas Community) - [Map](#)

Description:

One of the hardest problems with Infrastructure as Code tooling is modeling and managing complex relationships. This problem only becomes harder when multiple different tools are introduced, each lacking observability into the other. Then add build systems, application logic, deployments, CI/CD, and it becomes unbearably messy with footguns and CVEs around every corner.

At Exa, we take Nix far beyond building packages or development shells. Our entire infrastructure is modeled with Nix as one large DAG that allows us to manage these dependencies and orchestrate deployments across project boundaries with confidence in the process and its security. Join to learn more about Exa's introduction to Nix, how our usage has changed over time, how we think about flakes, and the lessons we've learned to build the future of search.

SpeakerBio: Ethan Carter Edwards

Ethan is a FLOSS advocate, longtime Nix user and contributor, and engineer. He's an active member of the Nixpkgs CUDA, Darwin, and NGI teams and is involved in various other efforts throughout the Nix ecosystem.

He currently works on building the infrastructure for the future of websearch at Exa.ai and studies Computer Science at Harvard University.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Your Lives are in Another Struct: Breaking Memory Hacks with Field Relocation

Tags: Game Hacking Village | Creator Talk/Panel

When: Friday, Aug 7, 14:45 - 15:45 PDT

Where: LVCCW Level 1 Hall 3 801 (Creator Stage 2) - [Map](#)

Description:

This talk introduces a compile time anti-cheat for Unity that leverages data-oriented properties of the Unity DOTS stack to move attacker targeted data across struct boundaries. Through static lifetime analysis and eligibility proofs, HP, Score, Lives, and more can be scrambled across a game at build-time, deeply challenging a motivated attacker.

SpeakerBio: Ryan Zmuda

Ryan is an incoming PhD student at Dartmouth College studying binary security and privacy. He is a published researcher with a special interest in program analysis, vulnerability triage, CI/CD security, and anti-cheat. At the University of Dayton he founded and led the Game Development Club, where he ran numerous seminars and speaker interviews alongside building an arcade cabinet from scratch. His pride and joy is yoyoengine, a 2D game engine written in C that he's been developing for three years.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Your OpSec Is Showing

Tags: Recon Village | Creator Talk/Panel

When: Saturday, Aug 8, 13:30 - 13:59 PDT

Where: LVCCW Level 1 Hall 3 801 (Creator Stage 2) - [Map](#)

Description:

Most threat intelligence focuses on what attackers have already done: payloads, malware families, and post-compromise behavior. But adversaries are far more fluid at the payload layer than they are at the infrastructure layer. Domains rotate, IPs churn, and malware gets recompiled but infrastructure leaves patterns.

This article explores how to track threat actors through their infrastructure by leveraging fingerprinting techniques that expose those patterns at scale.

We'll walk through practical methods including JARM for active TLS stack fingerprinting, JA3/JA4 for identifying consistent communication behaviors, SSH host key correlation for infrastructure pivoting, and MurmurHash for clustering phishing kits and web panels through shared assets. Individually, these signals are useful. Combined, they allow defenders to map infrastructure clusters tied to a single actor or campaign—even when traditional indicators change.

The focus is not on attribution for its own sake, but on building a repeatable approach to discovering “sister infrastructure” and identifying campaigns earlier in their lifecycle. By shifting attention away from payloads and toward the systems attackers stand up to operate, defenders can detect patterns before deployment and reduce time to awareness.

Attackers rely on reuse of configurations, tooling, and infrastructure. That reuse creates fingerprints. And those fingerprints are often more durable than the indicators most teams prioritize.

If you want to track threat actors effectively, stop chasing malware.

Track the infrastructure they can't help but reuse.

SpeakerBio: Fae Blu3Bird" Carlisle

Fae Carlisle (Blu3Bird) is a threat intelligence and DFIR practitioner working at the intersection of intelligence, detection, and threat hunting. She is an active member of hackers.town hacking community. Her work focuses on operationalizing intelligence, building systems and workflows that turn fragmented signals into actionable insights for real-world defense. She has experience developing intelligence pipelines and supporting detection efforts in production environments, with a focus on bridging the gap between analysis and response.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Your OTP Never Arrived: Attacking the Trust Boundary Where SMS Meets the Internet

Tags: DEF CON Official Talk | Demo | Exploit

When: Saturday, Aug 8, 11:30 - 12:30 PDT

Where: LVCCW Level 1 Hall 3 904 (Main Track 4) - [Map](#)

Description:

Kannel is the most widely deployed open-source SMS and WAP gateway in the world. With over 1000+ internet-facing instances across 65 countries, powering two-factor authentication, mobile banking, emergency alerts, and carrier-grade messaging, it forms a silent but critical pillar of global telecommunications infrastructure. Despite handling billions of messages, Kannel has received only a single CVE in its entire history. We present the results of a comprehensive security audit of Kannel SMS Gateway spanning versions 1.4.4, 1.4.5, and 1.5.0. Our research uncovered multiple previously unknown vulnerabilities. Most critically, we introduce telecom-specific attack primitives that exploit the inherent trust model between gateway components, enabling silent message censorship, billing fraud through forged delivery receipts, and audit evasion through metadata manipulation. These go beyond traditional memory corruption to expose fundamental design weaknesses in how SMS infrastructure routes, delivers, and accounts for messages. This talk fundamentally challenges the assumption that legacy telecom software is secure through obscurity.

<https://www.kannel.org/> <https://github.com/kannel> https://en.wikipedia.org/wiki/Short_Message_Peer-to-Peer
<https://www.kannel.org/doc.shtml> <https://gatewayapi.com/docs/apis/kannel/> <https://docs.smsportal.com/docs/kannel>
<https://github.com/playsms/book-playsms/blob/master/book-contents/en/Installation/Gateway-Installation/Kannel/Example-Kannel>
https://en.wikipedia.org/wiki/SMS_gateway <https://www.drupal.org/project/kannel> <https://smpp.org/>
<https://smpp.org/smpp-v5.html> <https://www.infobip.com/docs/essentials/api-essentials/smpp-specification>

Speakers: Kyprianos "kavasilo" Vasilopoulos, Nikos "nickvourd" Vourdas

SpeakerBio: Kyprianos "kavasilo" Vasilopoulos, Apifon

Kyprianos Vasilopoulos is a cybersecurity executive with 20+ years of experience in red teaming, incident response, penetration testing, and malware research. He is the CISO at Apifon and Co-Founder of OffensiveX. He has led cyber operations for major events like the Olympic Games and contributed to zero-day research at Trustwave SpiderLabs. Holding certifications such as OSCP and OSCE, he combines deep technical expertise with strategic leadership. His focus includes offensive security automation, red teaming, and threat-led penetration testing, and he has appeared on BBC News while being recognized in the Zyxel CVE Hall of Fame.

SpeakerBio: Nikos "nickvourd" Vourdas, EY

Nikos Vourdas, also known as nickvourd or NCV, is a Senior Offensive Security Consultant based in the US. With over five years of professional experience, he has actively participated in various global Tiber-EU and iCAST Red Teaming engagements. Nikos has conducted full Red Teaming operations to major clients across retail, banking, shipping, construction industries. He holds OSCE3, OSCP, OSWP, CRTL, CRT0 and OASP certifications. Also, he has previously presented at DEF CON, DevSecCon, and various BSides events around the world. Nikos loves contributing to open-source projects and always starts his day at 05:00 AM with a refreshing jog while listening to French rap music.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Your Packets Are Showing: Hybrid Quantum ML for Passive OS Fingerprinting

Tags: DEF CON Official Talk | Tool

When: Friday, Aug 7, 12:00 - 12:30 PDT

Where: LVCCW Level 1 Hall 3 1006 (Main Track 1) - [Map](#)

Description:

Quantum cybersecurity isn't just Q-Day. We took passive OS fingerprinting, the technique behind p0f and every modern ML-based fingerprinting tool, and mapped it onto a 20-qubit quantum circuit, replacing XGBoost as the classifier inside an "OsirisML"-style pipeline. Head-to-head on real packet captures from CIC-IDS 2017, the quantum version landed within 0.013 F1 of XGBoost on identical features, using roughly two orders of magnitude fewer trainable parameters. This is the first time a real DEF CON-relevant security workload has been mapped onto a quantum classifier with results that hold up against the classical tool the community already uses. The conversation about quantum and security has been stuck on cryptography. This talk is about everything else it can do.

M. Zalewski, "p0f v3," [Online]. Available: <https://lcamtuf.coredump.cx/p0f3/>. [Accessed: Apr. 25, 2026].

J. Holland, P. Schmitt, N. Feamster, and P. Mittal, "New Directions in Automated Traffic Analysis," in Proc. 2021 ACM SIGSAC Conf. on Computer and Communications Security (CCS), 2021, pp. 3366–3383, doi: 10.1145/3460120.3484758.

S. Ekeroth, J. Neale, and J. S. Kim, "Machine Learning Optimization for Enhanced OS Fingerprinting," Virginia Tech, 2024.

I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization," in Proc. 4th Int. Conf. on Information Systems Security and Privacy (ICISSP), 2018.

T. Chen and C. Guestrin, "XGBoost: A Scalable Tree Boosting System," in Proc. 22nd ACM SIGKDD Int. Conf. on Knowledge Discovery and Data Mining, 2016, pp. 785–794, doi: 10.1145/2939672.2939785.

M. Benedetti, E. Lloyd, S. Sack, and M. Fiorentini, "Parameterized quantum circuits as machine learning models," Quantum Sci. Technol., vol. 4, no. 4, p. 043001, 2019, doi: 10.1088/2058-9565/ab4eb5.

M. Schuld, A. Bocharov, K. M. Svore, and N. Wiebe, "Circuit-centric quantum classifiers," Phys. Rev. A, vol. 101, no. 3, p. 032308, 2020, doi: 10.1103/PhysRevA.101.032308.

K. Mitarai, M. Negoro, M. Kitagawa, and K. Fujii, "Quantum circuit learning," Phys. Rev. A, vol. 98, no. 3, p. 032309, 2018, doi: 10.1103/PhysRevA.98.032309.

M. Schuld, V. Bergholm, C. Gogolin, J. Izaac, and N. Killoran, "Evaluating analytic gradients on quantum hardware," Phys. Rev. A, vol. 99, no. 3, p. 032331, 2019, doi: 10.1103/PhysRevA.99.032331.

T. Jones and J. Gacon, "Efficient calculation of gradients in classical simulations of variational quantum algorithms," arXiv preprint arXiv:2009.02823, 2020.

H. Neven, V. S. Denchev, G. Rose, and W. G. Macready, "QBoost: Large scale classifier training with adiabatic quantum optimization," in Proc. Asian Conf. on Machine Learning (ACML), vol. 25, 2012, pp. 333–348.

V. Havlicek, A. D. Corcoles, K. Temme, A. W. Harrow, A. Kandala, J. M. Chow, and J. M. Gambetta, "Supervised learning with quantum-enhanced feature spaces," Nature, vol. 567, no. 7747, pp. 209–212, 2019, doi: 10.1038/s41586-019-0980-2.

M. Schuld and N. Killoran, "Quantum machine learning in feature Hilbert spaces," Phys. Rev. Lett., vol. 122, no. 4, p. 040504, 2019, doi: 10.1103/PhysRevLett.122.040504.

H. Suryotrisongko and Y. Musashi, "Evaluating hybrid quantum-classical deep learning for cybersecurity botnet DGA detection," *Procedia Comput. Sci.*, vol. 197, pp. 223–229, 2022, doi: 10.1016/j.procs.2021.12.135.

E. D. Payares and J. C. Martinez-Santos, "Quantum machine learning for intrusion detection of distributed denial of service attacks: a comparative overview," in *Proc. SPIE 11699, Quantum Computing, Communication, and Simulation*, 2021, p. 116990B, doi: 10.1117/12.2593297.

J. R. McClean, S. Boixo, V. N. Smelyanskiy, R. Babbush, and H. Neven, "Barren plateaus in quantum neural network training landscapes," *Nat. Commun.*, vol. 9, no. 1, p. 4812, 2018, doi: 10.1038/s41467-018-07090-4.

M. Cerezo, A. Sone, T. Volkoff, L. Cincio, and P. J. Coles, "Cost function dependent barren plateaus in shallow parametrized quantum circuits," *Nat. Commun.*, vol. 12, no. 1, p. 1791, 2021, doi: 10.1038/s41467-021-21728-w.

V. Bergholm et al., "PennyLane: Automatic differentiation of hybrid quantum-classical computations," *arXiv preprint arXiv:1811.04968*, 2018.

E. Grant, L. Wossnig, M. Ostaszewski, and M. Benedetti, "An initialization strategy for addressing barren plateaus in parametrized quantum circuits," *Quantum*, vol. 3, p. 214, 2019, doi: 10.22331/q-2019-12-09-214.

Speakers: Daniel Justice, Jae Sung Kim, La Alsulaim, Shreya G Savadatti

SpeakerBio: Daniel Justice, Carnegie Mellon University
No BIO available

SpeakerBio: Jae Sung Kim, Independent Researcher

Jae Sung Kim is an independent researcher specializing in network security and machine learning. His work focuses on applying novel computational approaches, including hybrid quantum-classical architectures, to classical security problems such as passive OS fingerprinting. He is a co-author of OsirisML, a machine learning pipeline for enhanced OS fingerprinting built on the nPrint packet representation framework.

SpeakerBio: La Alsulaim, University of Pittsburgh

La Alsulaim is a Computer Science student at the University of Pittsburgh. His research interests include machine learning applications

SpeakerBio: Shreya G Savadatti, Carnegie Mellon University

Shreya G Savadatti is a researcher specializing in quantum computing and cybersecurity. Currently a Master's student at Carnegie Mellon University, she explores Quantum Reservoir Computing (QRC) and cross-platform hardware benchmarking. As an IBM Qiskit Advocate, she contributes to open-source compilers and recently placed Top 5 at MIT iQuHACK 2026 for quantum circuit optimization. Her published research includes work on Quantum Fully Homomorphic Encryption (QFHE).



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Your Passkeys Won't Save You: Conditional Access Bypass via Auth-Method Downgrade

Tags: Red Team Village | Misc

When: Friday, Aug 7, 12:00 - 13:59 PDT

Where: LVCCW Level 1 Hall 1 309 (Red Team Village) Tactic Table 4 - [Map](#)

Description:

We rolled out passkeys" is the answer everyone gives now. So why does phishing still work? Because most tenants leave the password sitting there as a fallback method, and Conditional Access never closes the downgrade path. This workshop walks a Conditional Access test kit that proves it. You stand up a real domain with a valid certificate, fronted by nginx, and lure the victim into a browser that lives on your server. They see the real Microsoft login — no fake form — but when it offers a passkey, the kit clicks "sign in another way" and steers them to the password. If the tenant's CA allows that fallback, the victim completes a genuine login with a phishable factor and the kit harvests the tokens it issues — access, id, and refresh — server-side, then replays them into Microsoft Graph with no creds and no second factor. The whole point is the finding: can this tenant be downgraded, and what does the report say if it can't. We close on the CA configuration that actually shuts the downgrade path — and you run the kit yourself at the paired tactic.

Speakers: Doug Mooney, Jared Dobbelaer, Jon Rhodes

SpeakerBio: Doug Mooney

Doug Mooney (@dougmooney) leads offensive security at Blackbaud, running red team ops and building internal tooling to keep defenders honest. Previously an SVP at a major bank, he stood up their first internal pentest team and scaled offensive security across complex, regulated environments.

He focuses on adversary simulation, API abuse, and finding the weird edge cases that slip past detection. When he's not deep in a test, he's mentoring new talent, speaking at conferences, or still apologizing for that one time he "accidentally" reverse-synced LDAP in prod.

SpeakerBio: Jared Dobbelaer

Jared Dobbelaer (Fr13ndz) is an Adversarial Engineer at Blackbaud, conducting Red Team engagements and Penetration Testing in the Cloud.

Fr13ndz enjoys creative solutions that both help targets with organizational needs and requirements, while also borrowing their bearer tokens.

SpeakerBio: Jon Rhodes

Jon Rhodes is an Adversarial Engineer at Blackbaud and a member of the Synack Red Team (when he needs extra cash for new farm equipment).

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Your SaaS Is My Foothold: Weaponizing Shadow SaaS for Initial Access and Persistence

Tags: AppSec Village | Creator Event/Activity || All Audiences

When: Saturday, Aug 8, 16:30 - 17:30 PDT

Where: LVCCW Level 1 Hall 2 604 (Appsec Village) Arsenal - [Map](#)

Description:

Modern enterprise environments have shifted beyond traditional network perimeters, with SaaS applications and identity providers becoming the primary attack surface. However, a significant portion of this still remains unmanaged or invisible commonly referred as Shadow SaaS.

This session explores Shadow SaaS from an attacker's perspective, demonstrating how adversaries can identify, evaluate, and abuse unmanaged SaaS applications to gain initial access and maintain persistence within target environments.

Rather than focusing on inventory or governance, this talk reframes Shadow SaaS as an offensive opportunity. It highlights how implicit trust relationships, and third-party SaaS connections expand the attack surface beyond traditional security visibility.

Using the Shadow SaaS Surface Scanner, we demonstrate how attackers can uncover hidden SaaS exposure and leverage it as a foothold into enterprise environments.

SpeakerBio: Jordan Bonagura

Senior Security Consultant at Secure Ideas Researcher in Information Security Stay Safe Podcast Founder Computer Scientist Post Graduated in Business Strategic Management, Innovation and Teaching Founder - Vale Security Conference - Brazilian Conference Consultant Member - Brazilian Commission of High Tech Crime (OAB / SP) Coordinator and Teacher in IT area SJC Hacker Space President Speaker (DefCon, Hack Space Con, Hack Red Con, Hack Miami, Triangle InfoSec, AppSec California, GrrCon, BalCCCon2k14, BSides Augusta, H2HC, Angeles Y Demonios, Silver Bullet, Seginfo, ITA, INPE, etc)



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Your WAF Blocked Us, That Was The Exploit - Remote Agent Takeover via Cloudflare, Sentry and Claude Zero-Day for data exfil

Tags: DEF CON Official Talk | Demo | Exploit

When: Sunday, Aug 9, 12:00 - 12:59 PDT

Where: LVCCW Level 1 Hall 3 1006 (Main Track 1) - [Map](#)

Description:

What happens when getting blocked by your WAF is exactly how the attacker gets in? We built two new remote exploit chains that hijack AI agents through Cloudflare and Sentry - two of the most trusted tools on the internet. No malware. No binary exploits. The attacker never touches the victim or their agent. Just text in public logs, waiting to be read. Chain 1: We send requests Cloudflare blocks with 403 - and that is the attack. Our payloads land in WAF logs. When a dev asks their agent to debug Cloudflare, injections activate via cloudflare queries. Using only Cloudflare's own MCP tools, we hijack DNS and reroute customer traffic. Chain 2: We inject stacktraces into Sentry's public API, no auth needed. Sentry's "Seer" agent reads them, gets compromised, and its poisoned recommendations flow into a developer's Cursor which executes our commands. One agent infecting another. First demo of agent-to-agent lateral movement and "Self-Exploiting Agent" technique. Then we go deeper: a zero-day in Claude bypasses its network sandbox for full data exfiltration. For persistence, we show how "agentic rootkits" work by memory injection and config poisoning, invisible to EDRs. est 15,000+ organizations exposed via Cloudflare MCP alone. 27% of them are Fortune 1000. Responsibly disclosed. We're now showing everything.

*Cloudflare MCP Server documentation and public deployment *Sentry MCP Server and Seer AI agent documentation

*Anthropic Claude Desktop application architecture *Cursor AI coding agent - MCP integration and tool architecture

*OWASP Top 10 for LLM Applications (2025) *MITRE ATLAS - Adversarial Threat Landscape for AI Systems

*Clinejection (Feb 2026) - GitHub issue title exploit compromising Cline's release pipeline *Comment & Control (Apr 2026) - prompt injection via PR titles leaking secrets from Claude Code, Gemini CLI, and Copilot

Speakers:Barak Sternberg,Nevo Poran,Ron Bobrov

SpeakerBio: Barak Sternberg, Tenet Security

Barak Sternberg is a cybersecurity researcher, offensive security specialist, and a returning DEFCON speaker. His research career spans over 15 years across every major attack surface of the last decade: from IoT to browser extension exploits (DEFCON 29), to Kube infra attacks (with Nevo), to smart device hacking (DEFCON Safe Mode IoT Village). He's presented at DEFCON (twice), Hacktivity, RootCon, BSides, Intent, and numerous other security conferences worldwide. He's a Unit 8200 veteran and Israel Defense Prize recipient. His research has consistently focused on finding novel attack chains in emerging technology before attackers do, across years in offensive cybersecurity. He also co-founded Wild Pointer (offensive security, Fortune 500 clients) and more recently co-founded Tenet Security as CEO with Nevo: but the research came first, the company came from the research, not the other way around. He leads Tenet while staying hands-on - the exploit chains in this talk came directly from his team's research

SpeakerBio: Nevo Poran

Nevo Poran, cybersecurity researcher, Co-Founder & CTO of Tenet Security, and a top-tier security engineer focused on GenAI, API, and application security. Unit 8200 veteran and 2x Excellence Awards. Nevo co-founded Wild Pointer with Barak, serving as technical lead and later CEO, managing teams delivering offensive R&D to Cisco, Nonym Security, and Fortune 500 clients. He then co-led Cisco's first GenAI Security Research Team - building the AI Defense product from research through production. Deep hands-on expertise in reverse engineering, exploit development, and agent runtime security. Speaks on Kubernetes/cloud and GenAI security (CyberArk INTENT 2024, UNC Symposium 2025) and co-presented the Kubernetes etcd exploitation research with Barak. They've been breaking things together for years.

SpeakerBio: Ron Bobrov, Tenet Security

Ron Bobrov is a senior security researcher at Tenet Security with 10 years of experience in offensive security, penetration testing, and vulnerability research. He has specialized in emerging attack vectors and has recently focused on AI agent security, conducting red-team assessments that have uncovered critical vulnerabilities in modern LLM-based systems. At Tenet Security, Ron leads research initiatives exploring the intersection of traditional security threats and AI-specific attack surfaces. His work on bypassing A2AS framework protections has revealed fundamental architectural gaps in current AI agent security approaches, contributing to the development of runtime protection methodologies for agentic systems. Ron's research combines deep technical expertise in system exploitation with novel approaches to adversarial AI security, helping organizations understand and defend against the next generation of attacks targeting AI agents in production environments.



[Return to Index](#) - Add to Google - ics [Calendar](#) file

Title: Zealot: An Autonomous Cloud Offensive Multi-Agent System

Tags: AI | DEF CON Demo Labs | Intermediate | AppSec | Cloud | Defense/Blue Team | Offense/Red Team | Purple Team | SecOps | DEF CON Demo Labs

When: Friday, Aug 7, 11:00 - 11:45 PDT

Where: LVCCW Level 1 Hall 3 900 (Demo Labs Track 4) - [Map](#)

Description:

In November 2025, Anthropic disclosed a state-sponsored operation where AI didn't assist human attackers — it was the attacker, executing 80-90% of the campaign autonomously. The question shifted from "could this happen?" to "how bad can it get?"

We built Zealot to find out.

Zealot is a multi-agent offensive framework that autonomously chains reconnaissance, exploitation, privilege escalation, and data exfiltration against cloud environments — with no human directing individual steps. A supervisor agent coordinates three specialists (Infrastructure, AppSec, and Cloud) that share attack state and hand off context as the operation progresses. The result: an AI system that thinks strategically and executes tactically, the way a real red team does.

In live sandbox tests against GCP, Zealot autonomously discovered an exposed web service, identified and exploited an SSRF vulnerability, extracted service account credentials from the metadata service, impersonated a higher-privileged account, and exfiltrated BigQuery datasets — start to finish, without a human touching the keyboard after the objective was set.

We'll walk through the architecture, show the full attack chain on video, and share the honest lessons: where AI operators excel (systematic enumeration, credential chaining, API fluency), where they fall short (a

SpeakerBio: Chen Doytshman

I'm a security researcher with a background in artificial intelligence and machine learning. I am passionate about using my skills to protect against cyber threats. With over 5 years of experience in the field, I have a strong understanding of both security and AI technologies and am skilled at combining the two to identify and mitigate vulnerabilities.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Zealot: An Autonomous Cloud Offensive Multi-Agent System

Tags: AI | DEF CON Demo Labs | Intermediate | AppSec | Cloud | Defense/Blue Team | Offense/Red Team | Purple Team | SecOps | DEF CON Demo Labs

When: Saturday, Aug 8, 12:00 - 12:45 PDT

Where: LVCCW Level 1 Hall 3 900 (Demo Labs Track 4) - [Map](#)

Description:

In November 2025, Anthropic disclosed a state-sponsored operation where AI didn't assist human attackers — it was the attacker, executing 80-90% of the campaign autonomously. The question shifted from "could this happen?" to "how bad can it get?"

We built Zealot to find out.

Zealot is a multi-agent offensive framework that autonomously chains reconnaissance, exploitation, privilege escalation, and data exfiltration against cloud environments — with no human directing individual steps. A supervisor agent coordinates three specialists (Infrastructure, AppSec, and Cloud) that share attack state and hand off context as the operation progresses. The result: an AI system that thinks strategically and executes tactically, the way a real red team does.

In live sandbox tests against GCP, Zealot autonomously discovered an exposed web service, identified and exploited an SSRF vulnerability, extracted service account credentials from the metadata service, impersonated a higher-privileged account, and exfiltrated BigQuery datasets — start to finish, without a human touching the keyboard after the objective was set.

We'll walk through the architecture, show the full attack chain on video, and share the honest lessons: where AI operators excel (systematic enumeration, credential chaining, API fluency), where they fall short (a

SpeakerBio: Chen Doytshman

I'm a security researcher with a background in artificial intelligence and machine learning. I am passionate about using my skills to protect against cyber threats. With over 5 years of experience in the field, I have a strong understanding of both security and AI technologies and am skilled at combining the two to identify and mitigate vulnerabilities.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Zero Day Hire: Can You Spot the Spy?

Tags: Social Engineering Community Village | Creator Event/Activity

When: Friday, Aug 7, 13:30 - 14:30 PDT

Where: LVCCW Level 3 W320 (Social Engineering Community Village Labs) - [Map](#)

Description:

If your hiring process relies solely on traditional background checks, you're already behind. You think you're hiring a Senior Backend Engineer. You've reviewed the resume, passed the technical interview, and cleared the automated background check. But you've actually just handed a corporate laptop to a spy.

This 60-minute workshop puts the attendee in the seat of an OSINT lead during a live-fire exercise. This isn't a lecture; it's a test to stop a breach before it starts. Attendees will be provided with the same "evidence" a recruiter would see, and the goal is simple: perform a background check to identify fake personas. You have 60 minutes. Can you do it?

Key Takeaways: - Learn why standard background checks miss AI-generated personas and synthetic identities - Leave with a practical, legally-conscious verification process you can use by Monday morning

Note: Please bring your own laptop. Attendees should be comfortable installing and using common OSINT tools to participate in the live investigation.

Speakers: Michael Reimsbach, Rishi "rxerium" C

SpeakerBio: Michael Reimsbach, Product Security Specialist at SAP

Michael is a Product Security Specialist at SAP, working with the SAP Cloud Infrastructure security team. His focus areas include vulnerability management, secrets management, and building secure internal services.

He obtained multiple industry certifications such as OSCP, GCPN, and CISSP.

A healthy dose of paranoia led him to explore OSINT and the surprising power of publicly available information.

Beyond his day-to-day work, Michael is an active member of the cybersecurity community and helps organize BSides Luxembourg.

SpeakerBio: Rishi "rxerium" C, Security Researcher

Rishi is a London-based security researcher with over five years of hands-on experience in IT. He currently specializes in vulnerability research, threat intelligence, and enterprise risk analysis. His current focus lies in identifying and analyzing zero-day vulnerabilities and emerging CVEs, often working to reverse engineer exploit mechanics and build detection logic before public weaponization. Rishi's work spans both offensive and defensive domains—developing threat models based on real-world TTPs, crafting custom detection rules, and automating reconnaissance pipelines to uncover exploitable misconfigurations and exposed assets. He is particularly active in attack surface management (ASM) and OSINT, where he leverages DNS enumeration, passive data correlation, and large-scale infrastructure scanning to surface unknown entry points and map adversary-accessible exposure. Outside of research, Rishi integrates findings into operational tooling and supports data-driven prioritization strategies to bridge technical risk and business impact. His work reflects a deep commitment to adversary-informed defense and proactive discovery across modern hybrid environments.



Title: Zero Day Hire: Can You Spot the Spy?

Tags: Social Engineering Community Village | Creator Event/Activity

When: Friday, Aug 7, 12:00 - 12:59 PDT

Where: LVCCW Level 3 W320 (Social Engineering Community Village Labs) - [Map](#)

Description:

If your hiring process relies solely on traditional background checks, you're already behind. You think you're hiring a Senior Backend Engineer. You've reviewed the resume, passed the technical interview, and cleared the automated background check. But you've actually just handed a corporate laptop to a spy.

This 60-minute workshop puts the attendee in the seat of an OSINT lead during a live-fire exercise. This isn't a lecture; it's a test to stop a breach before it starts. Attendees will be provided with the same "evidence" a recruiter would see, and the goal is simple: perform a background check to identify fake personas. You have 60 minutes. Can you do it?

Key Takeaways: - Learn why standard background checks miss AI-generated personas and synthetic identities - Leave with a practical, legally-conscious verification process you can use by Monday morning

Note: Please bring your own laptop. Attendees should be comfortable installing and using common OSINT tools to participate in the live investigation.

Speakers: Michael Reimsbach, Rishi "rxerium" C

SpeakerBio: Michael Reimsbach, Product Security Specialist at SAP

Michael is a Product Security Specialist at SAP, working with the SAP Cloud Infrastructure security team. His focus areas include vulnerability management, secrets management, and building secure internal services.

He obtained multiple industry certifications such as OSCP, GCPN, and CISSP.

A healthy dose of paranoia led him to explore OSINT and the surprising power of publicly available information.

Beyond his day-to-day work, Michael is an active member of the cybersecurity community and helps organize BSides Luxembourg.

SpeakerBio: Rishi "rxerium" C, Security Researcher

Rishi is a London-based security researcher with over five years of hands-on experience in IT. He currently specializes in vulnerability research, threat intelligence, and enterprise risk analysis. His current focus lies in identifying and analyzing zero-day vulnerabilities and emerging CVEs, often working to reverse engineer exploit mechanics and build detection logic before public weaponization. Rishi's work spans both offensive and defensive domains—developing threat models based on real-world TTPs, crafting custom detection rules, and automating reconnaissance pipelines to uncover exploitable misconfigurations and exposed assets. He is particularly active in attack surface management (ASM) and OSINT, where he leverages DNS enumeration, passive data correlation, and large-scale infrastructure scanning to surface unknown entry points and map adversary-accessible exposure. Outside of research, Rishi integrates findings into operational tooling and supports data-driven prioritization strategies to bridge technical risk and business impact. His work reflects a deep commitment to adversary-informed defense and proactive discovery across modern hybrid environments.



Red Team Village - Friday - 10:00-11:59 PDT

Title: Zero Signal: Operating Where Defenders Can't See

Tags: Red Team Village | Misc

When: Friday, Aug 7, 10:00 - 11:59 PDT

Where: LVCCW Level 1 Hall 1 309 (Red Team Village) Tactic Table 3 - [Map](#)

Description:

82% of intrusions in 2025 involved no malware — adversaries operated through valid credentials, cloud APIs, and identity abuse, generating zero endpoint signal. Cloud-conscious intrusions surged 37% year-over-year, with groups like Storm-2372, Midnight Blizzard, and Scattered Spider executing major breaches using only OAuth tokens and cloud management APIs — no payloads, no processes, no EDR alerts. Yet the average cloud breach takes 143 days to detect, and 45% are discovered by external parties, not internal teams. This tactic puts participants in that detection dark space. Using Stratus Red Team and CloudGoat in pre-provisioned cloud environments, attendees execute end-to-end attack chains across AWS and Azure that produce no endpoint telemetry. No prior cloud experience required; guided walkthroughs and command references provided.

Outline:

Phase 1 — Cloud Recon & IAM Enumeration (10 min): Participants enumerate IAM permissions, map trust relationships, and identify exploitable default service roles using Pacu and CLI tools. Learn how to fingerprint an organization's cloud telemetry posture before executing.

Phase 2 — Privilege Escalation via Default Roles (15 min): Exploit overpermissioned default IAM roles (SageMaker S3 Glue pathway documented in Aqua Security research). Participants escalate from a low-privilege user to cross-service access using only cloud API calls — zero endpoint involvement.

Phase 3 — Lateral Movement & Exfiltration (15 min): Move laterally through cloud management planes using SSM sessions, cross-account role assumption, and EBS snapshot theft. Exfiltrate data through VPC endpoints — a known CloudTrail blind spot where data events are not logged.

Phase 4 — Persistence & Detection Review (10 min): Establish persistence via OAuth application backdoors and rogue service principals. Then flip to the defender's view: examine what CloudTrail, GuardDuty, and Entra ID audit logs actually captured versus what they missed entirely.

Attendees walk away with: - A repeatable cloud-native attack methodology that avoids all endpoint detection - Hands-on experience with Stratus Red Team, CloudGoat, and Pacu - A practical map of CloudTrail, GuardDuty, and audit log blind spots - Understanding of which cloud operations generate telemetry and which don't

SpeakerBio: Gowthamaraj Rajendran

Gowthamaraj Rajendran is a cybersecurity professional and Threat Detection Engineer with 6+ years of experience, specializing for the last 3 years in creating precise and effective detection capabilities.

[Return to Index](#) - Add to Google  - ics [Calendar](#) file

Title: Zero Trust Kubernetes Security: Preventing Real World Container Attacks

Tags: Intermediate | AppSec Village | Creator Talk/Panel

When: Friday, Aug 7, 15:30 - 15:59 PDT

Where: LVCCW Level 1 Hall 2 604 (Appsec Village) Main Stage - [Map](#)

Description:

Kubernetes has become a major application attack surface, where most breaches exploit misconfigurations and implicit trust rather than software flaws. This session presents a practical Zero Trust approach to securing containerized applications against real world attack paths. It shows how attackers abuse weak RBAC, insecure service communication, and lack of workload isolation to move laterally and escalate privileges. Attendees will learn how to design granular access controls, enforce secure service to service communication, and implement segmentation to contain compromised workloads. The session also demonstrates how policy as code and admission controls can block risky deployments before they reach production. With real examples and measurable outcomes, this talk provides actionable techniques to reduce attack success and strengthen Kubernetes security.

SpeakerBio: Janakiram Meka

Janakiram Meka is a Cloud DevOps Architect with over 18 years of experience in building and securing large scale enterprise systems. His expertise spans cloud infrastructure, Kubernetes, DevSecOps, and Zero Trust security models. He has led cloud migration and automation initiatives across complex environments, focusing on improving security, scalability, and operational efficiency. Janakiram holds multiple industry certifications, including Kubernetes Administrator, Terraform Associate, Oracle Certified Professional, and AWS Solutions Architect. He is an active contributor to the technology community, writing technical articles on cloud and database systems, and is a Senior Member of IEEE. His work emphasizes practical, data driven approaches to securing modern application platforms.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Zero-Cloud Threat Modeling: Vector Embedding Architectures for Automated Vulnerability Detection

Tags: AI | DEF CON Demo Labs | Intermediate | AppSec | Threat Intel/Hunting | DEF CON Demo Labs

When: Friday, Aug 7, 13:00 - 13:45 PDT

Where: LVCCW Level 1 Hall 3 900 (Demo Labs Track 4) - [Map](#)

Description:

Traditional threat modeling is a tedious, manual process prone to human error. Conversely, modern "AI" threat modeling tools almost universally depend on sending sensitive, proprietary system architectures to third-party APIs in cleartext.

We present AI Threat Modeler (AITM), a fully open-source, zero-cloud application designed to automate architecture-driven STRIDE threat modeling completely offline. AITM fundamentally shifts how we analyze system designs by replacing brittle, keyword-based regex rules with a local Semantic AI Engine.

Under the hood, AITM leverages sentence-transformers and an in-memory FAISS vector database to embed a comprehensive, 116+ component knowledge base. During analysis, a custom NetworkX graph builder parses natural language or structured architecture descriptions (via spaCy) to map undocumented architectural features to known CVE classes and STRIDE categories.

Furthermore, AITM introduces "Architecture Intelligence" using graph traversal algorithms to automatically infer missing trust boundaries and identify multi-step attack chains that standalone component scanning misses. In this demo, we will: Walk through the automated ingestion of a microservice architecture. Demonstrate how the local FAISS engine discovers semantic threats that evade keyword matching. Show dynamic attack cha

SpeakerBio: Ankit Vashisth

Ankit Vashisth is a Security Engineer with over 4 years of experience in application security, cloud security, and DevSecOps. He has worked on security assessments across web, mobile, network, and enterprise systems for global clients. His interests include AI-driven security tooling, threat modeling, and security automation. Ankit actively researches ways to apply AI to improve security architecture analysis and vulnerability detection.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Zero-Cloud Threat Modeling: Vector Embedding Architectures for Automated Vulnerability Detection

Tags: AI | DEF CON Demo Labs | Intermediate | AppSec | Threat Intel/Hunting | DEF CON Demo Labs

When: Saturday, Aug 8, 16:00 - 16:45 PDT

Where: LVCCW Level 1 Hall 3 900 (Demo Labs Track 4) - [Map](#)

Description:

Traditional threat modeling is a tedious, manual process prone to human error. Conversely, modern "AI" threat modeling tools almost universally depend on sending sensitive, proprietary system architectures to third-party APIs in cleartext.

We present AI Threat Modeler (AITM), a fully open-source, zero-cloud application designed to automate architecture-driven STRIDE threat modeling completely offline. AITM fundamentally shifts how we analyze system designs by replacing brittle, keyword-based regex rules with a local Semantic AI Engine.

Under the hood, AITM leverages sentence-transformers and an in-memory FAISS vector database to embed a comprehensive, 116+ component knowledge base. During analysis, a custom NetworkX graph builder parses natural language or structured architecture descriptions (via spaCy) to map undocumented architectural features to known CVE classes and STRIDE categories.

Furthermore, AITM introduces "Architecture Intelligence" using graph traversal algorithms to automatically infer missing trust boundaries and identify multi-step attack chains that standalone component scanning misses. In this demo, we will: Walk through the automated ingestion of a microservice architecture. Demonstrate how the local FAISS engine discovers semantic threats that evade keyword matching. Show dynamic attack cha

SpeakerBio: Ankit Vashisth

Ankit Vashisth is a Security Engineer with over 4 years of experience in application security, cloud security, and DevSecOps. He has worked on security assessments across web, mobile, network, and enterprise systems for global clients. His interests include AI-driven security tooling, threat modeling, and security automation. Ankit actively researches ways to apply AI to improve security architecture analysis and vulnerability detection.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Zero-Day Provisioning: Chaining TP-Link ZTP Vulnerabilities for Infiltrating Networks

Tags: DEF CON Official Talk | Demo | Exploit

When: Saturday, Aug 8, 15:30 - 16:30 PDT

Where: LVCCW Level 1 Hall 3 1007 (Main Track 2) - [Map](#)

Description:

Today network equipment vendors offer Zero-Touch Provisioning (ZTP) for configuring devices with little-to-no manual intervention. However, it is often taken for granted that the networking protocols used in ZTP are secure.

Most vulnerability and threat intelligence reports on network equipment focus on individual “device takeover” vulnerabilities allowing for direct Remote Code Execution. Yet, there is little recent research examining the security of ZTP designs and implementations, where the exploitation impact may be on a much larger scale.

In this talk, we will present 17 vulnerabilities affecting TP-Link Omada – a device ecosystem designed with ZTP in mind. We will present the Omada protocols ZTP and discuss key vulnerabilities in them, including a chain of trust compromise due to the use of hard-coded cryptographic keys, sensitive information disclosure, and remote code execution against some devices.

We will present attacks against controllers and client devices that allow attackers to infiltrate networks by taking over Omada equipment. We will also show that some of the issues go way beyond one device family and affect other network equipment, security cameras, smart home devices, and mobile apps with millions of downloads.

Speakers: Francesco La Spina, Stanislav Dashevskiy

SpeakerBio: Francesco La Spina, Forescout Technologies

Francesco La Spina holds an MSc in Computer Science from the University of Trento, Italy. He began his career as a software engineer with a focus on IT/IoT security gateway development, honing his expertise in crafting robust security solutions for digital infrastructures. Having served as a security engineer for an ISP and financial institutions, he also gained invaluable experience in fortifying networks against potential threats. Currently, Francesco is engaged in cutting-edge security research and threat analysis within the realms of IT and IoT at Forescout Technologies - Vedere Labs.

SpeakerBio: Stanislav Dashevskiy, Forescout Technologies

Stanislav Dashevskiy is a Security Researcher at Forescout. He received his PhD from the International Doctorate School in Information and Communication Technologies (ICT) at the University of Trento (Italy) in 2017. His main research interests are open source software, software security, and vulnerability analysis.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

Title: Zero-Knowledge Unsaflok: The Unsaflok Saga Continues

Tags: Physical Security Village | Creator Talk/Panel

When: Saturday, Aug 8, 16:00 - 16:59 PDT

Where: LVCCW Level 1 Hall 3 1104 (Creator Stage 4) - [Map](#)

Description:

Continuing the legacy of the previous two Unsaflok research teams, we expanded the original Unsaflok attack to a zero-knowledge exploit by mimicking the HH6 maintenance unit's lock interrogation protocol. The HH6 is normally used by hotel staff to diagnose lock errors and problems, but it also has the capability to retrieve the Property ID from the lock. Previously, a hotel card from the property was required to perform the exploit as the cards were the only way to get the Property ID value, but replicating the HH6 protocol to directly extract the necessary information directly from the lock removes this limitation. After messing with voltage glitching and EMFI for HH6 firmware recovery, we dug into the binaries to produce an extremely fast, zero knowledge, undetectable Unsaflok attack using a Flipper Zero.

Speakers: Ben Higgins, Aaron Tulino

SpeakerBio: Ben Higgins, Embry-Riddle Aeronautical University, Prescott Campus

Ben is an undergraduate at Embry Riddle Aeronautical University Prescott Campus, and is very new to this kind of security research. He spends most of his time in this field researching access control and RFID.

SpeakerBio: Aaron Tulino, Embry-Riddle Aeronautical University, Prescott Campus

Aaron is an undergraduate at Embry Riddle Aeronautical University Prescott Campus. He has experience in reverse engineering, software development, and software security, but is relatively new to the RFID field.

[Return to Index](#) - Add to Google



- ics [Calendar](#) file

The wait is over. Meet the DEF CON 34 badge!

Posted 2026-07-31

It's the creation of hardware superstar [Bunnie Huang](#), and it features his open-source, fully inspectable Baochip.

DEF CON 34 badgeholders will be the first to get their hands on a radically transparent device with all kinds of powerful possibilities - security token, password manager, HSM, pretty light generator - that we hope will keep you busy long after closing ceremonies.

What will you make with yours?

[More in this story on Wired !](#)

No Recording Glasses at DEF CON 34

Posted 2026-07-28

Meta style glasses with recording capabilities are prohibited at DEF CON. Surreptitious filming is an invasion of privacy, and will be treated as a CoC violation. There is no exception for recording glasses with prescription lenses. Be sure to pack non-violating eyewear if you need them.

If you must take pictures, use recognizable personal photo equipment like a smartphone so that your intentions are clear. Get affirmative permission from the faces in your frame. Please refer to our official [Photo](#) and [code of conduct](#) policies for more.

DEF CON Middle East Postponed

Posted 2026-07-24

The safety of our community is our highest priority.

For this reason, we have decided to postpone DEF CON Middle East. The evolving security situation in the region makes it impossible to concentrate on delivering the experience attendees deserve.

We understand that this news is disappointing, but we believe it's the most responsible choice right now. We look forward to bringing the full DEF CON experience to friends new and old in Bahrain, and we will share new dates and information as soon as they are confirmed.

In the meantime, we'd like to offer our sincere thanks to the community, sponsors, and supporters for their understanding and continued trust. We hope and expect to welcome you to DEF CON Middle East soon, under better circumstances for everyone.

-The DEF CON Middle East Team

Workshops Page is Live! Reg Opening Soon!

Posted 2026-07-10

Prepare yourselves! DEF CON 34 Workshop registration goes live at noon PDT on July 14! First come, first served.

The [full course lineup](#) is available on the [DEF CON site](#) .

Make sure to limber up your clicking mechanism of choice and stay hydrated.

Godspeed and good luck to all of you!

DEF CON Room Blocks: Only a Week Left!

Posted 2026-07-07

The DEF CON room blocks at the Wynn and Encore are now sold out. You can still get a block discount at these three hotels:

[Embassy Suites](#)

[Spring Hill Suites](#)

[Renaissance](#)

The special rates are only available until July 15, so act expeditiously.

Less than a month to go! Are you ready?

DC34 Lodging update!

Posted 2026-06-24

We've got three more hotels where you can get a DEF CON discount, **but you need to book quickly** ! We have blocks at:

[Spring Hill Suites](#)

Or call (702) 433-5880

[Embassy Suites](#)

Or call (702) 893-8000

[Renaissance](#)

Or call (702) 784-5700

Book by July 15 for the special rate!

See you soon!

DEF CON 34 Music Announcement!

Posted 2026-06-09

They have been selected. [These are the mighty masters of groove charged with keeping your rumps shaking at DEF CON](#) . We salute them and look forward to their musical service.

Let's GoOo!

DEF CON 34 Badge Alert: SAO Edition

Posted 2026-05-20

DEF CON 34 is an electronic badge year, and we've got something very special in store, created for us by a hardware hacking legend. We can't share too much at this juncture, but we can say this: it will be iconic. First round Hall of Fame. In addition to being a cool badge, it's a platform. It's a full-fledged, first-of-its-kind inspectable platform. Long after closing ceremonies we think you'll still be using this device to regain some agency and security in this rapidly complexifying world.

So what we can offer right now is some data to help all the SAO enthusiasts out there. Please enjoy this [spec sheet](#) with the relevant schematics, measurements and clearances for your projects. Electro-specs also included.

We're excited to see what you come up with. As good as the badge is, we know you can make it better.

DEF CON Middle East Update

Posted 2026-05-19

It's official - the papers are signed and DEF CON Middle East is on track for November 11-12, 2026 in Bahrain! There will also be a full slate of DEF CON 2-day Trainings available November 8-10. After a very successful mini-con at last year's Arab International Cybersecurity Conference, we look forward to bringing the full DEF CON experience to Bahrain and the region. Stay tuned to these channels for updates, and save the date.

[The press release is here](#)

DEF CON 34 Hotel Update

Posted 2026-05-07

Spring has sprung. DEF CON planning season is in full swing, and our discounted room blocks are filling up fast. If you've been waiting for a sign to lock down your booking, this is probably it.

The DEF CON room block at the Fountainebleau is officially sold out. [Special DEF CON rates are still available at Encore](#)

and Wynn , so get those while they last.

August will be here before you know it. Are you ready?

DEF CON in the News: Singapore edition

Posted 2026-05-04

Our founder, The Dark Tangent, did a live interview on CNA. It's worth your time.

<https://www.youtube.com/watch?v=9-qKcofJvy8>

DEF CON Middle East Call for Trainers

Posted 2026-04-22

We're excited to announce that the [Call for Trainers is now OPEN for DEF CON Training Middle East](#) !

Are you passionate about cybersecurity, hacking, and hands-on learning? Do you have expertise in emerging threats, defensive strategies, or cutting-edge security techniques? We want to hear from you!

Visit training.defcon.org to submit your trainer application for a two-day or three-day course by May 9, 2026.

DEF CON Singapore Talks!

Posted 2026-04-06

You can now find the [full list of speakers online](#) !

It's always a good idea to plan ahead. Make sure you don't miss the talks that matter most to you. If you need tickets, [visit our shop](#) .

Just a few weeks away now. We can't wait to see everyone!

DEF CON Training Las Vegas Course Lineup is Live!

Posted 2026-04-04

DEF CON Training Las Vegas 2026 Course Lineup is now live!

We're thrilled to share the full slate of courses for DEF CON Training in Las Vegas! Join us in August for hands-on courses led by top practitioners from across the community.

For the first time ever, we will offer 1-day, 2-day, and 4-day classes! Whatever your needs, whether you're sharpening fundamentals or diving deep into advanced techniques, there's something here for you!

Explore the full lineup and course details here: <https://training.defcon.org/>

Explore our offerings, grab your seat, and get ready to learn and build.

Call for Hosts: Hacker Jeopardy at DEF CON Singapore

Posted 2026-03-18

We are looking for charismatic, quick-witted, and tech-savvy individuals to take the stage as hosts of DEF CON's Hacker Jeopardy Singapore! If you have a knack for command-line humor, a deep well of cybersecurity trivia, and the ability to keep a rowdy room of hackers entertained, we want to hear from you.

This isn't your average trivia night. As a host, you will:

- **Local Presence:** Ideally based in or able to travel to Singapore for the event, with a deep understanding of local hacker history and references.
- **Command the Room:** Moderate the game with energy, keeping the pace fast and the vibes high. Bring your own flair—whether it's dry wit, high energy, or niche infosec references.
- **Technical Literacy:** You should know your nmap from your netcat and your 0-days from your Old-days. Use your technical background to judge answers on the fly (and maybe engage in some light-hearted debate over technicalities).
- **Public Speaking & Improv Experience:** Comfort behind a microphone and in front of a crowd is essential. The ability to handle technical glitches or spicy contestants with grace and humor.

How to Apply

If you're ready to be the face of Hacker Jeopardy Singapore, please send us a brief message including:

1. A short "Elevator Pitch": Why are you the perfect host?
2. Your "Technical Niche": What's the one topic you could write an entire Jeopardy category about?
3. Experience: Any links to previous talks, hostings, or even a 30-second "demo" clip of your hosting persona.

Deadline: 2026-04-02

Apply at: Contests@defcon.org

DEF CON Middle East Dates!

Posted 2026-03-13

We've got dates for this year's event in Bahrain!

Following a very successful event in 2025, DEF CON and DEF CON Training are returning to Bahrain for DEF CON Middle East.

Training will be held November 8-10 and DEF CON Middle East will be November 11-12.

We hope you'll save the date and follow us for updates.

DEF CON 34 Theme!

Posted 2026-03-10

DEF CON 34's theme is 'Agency'. We're focusing on self-determination in our use of tech. Charting our own course and helping others do the same. Let's start moving our valuable attention to tech that supports our agency. Let's find the places we can help and choose to act. Read more at: <https://defcon.org/html/defcon-34/dc-34-theme.html> Visual style guide and homework assignments coming soon!

DEF CON 34 Pre-Registration is Open!

Posted 2026-03-04

The wait is over. [Pre-registration for DEF CON 34](#) opens TODAY!

Reminder – the cash route is unchanged: Cash at the door registration (LineCon) will continue in its traditional, vibey fashion (think hacker slumber party). Doors open Thursday, August 6 and the price is \$520.

Those who pre-register are guaranteed a human badge, even if we run out. To receive this badge, you must redeem your ticket onsite. The badge entitles one human full access to the DEF CON floor during open hours. Tickets are fully transferrable, so which human gets that access is up to the purchaser.

Pre-reg is open at shop.defcon.org until July 31 at 8:59 PM EDT. After that date registration is LineCon only. If you have any questions or need to make bulk purchases please email us at info@defcon.org.

There are some pricing benefits to early registration, too. Early bookers save money, so don't procrastinate. August will be here before you know it.

Ticket Pricing:

Early Bird - \$560 (\$540 + \$20 CC Processing Fee) - Good until May 22 at 8:59pm EDT

Regular - \$580 (\$560 + \$20 CC Processing Fee) - Good from May 23 to July 17 at 8:59pm EDT

Late - \$600 (\$580 + \$20 CC Processing Fee) - Good from July 18 to July 31 at 8:59pm EDT

Ticket Cancellation Fee:

Before July 18 - \$34

After July 18 - \$84

Check out the following for villages, contests, and communities accepted to return this year:

[Villages](#)

[Contests](#)

[Communities](#)

Introducing the New DEF CON CTF Organizers: Benevolent Bureau of Birds!

Posted 2026-03-03

Back in 1996 at DEF CON 4, the first Capture The Flag contest was created. It build on the chaos of a wide open network at DC 3, and has continued to be the premier computer security CTF contest.

The CTF started with a single person watching over it and turned into a team effort. Soon teams of hackers and past CTF players would become organizers, building on those that came before while continuing to push the edge of what's possible.

Today things are changing fast, with agentic tools shaking up the industry. This change has already been reflected in the CTF space. At DEF CON 33 CTF, Sampriti of the team Blue Water discovered that their agentic tool had completed a challenge only after a judge notified them that they had already won. It was an exciting novelty.

This year, we expect that novelty to be the norm.

For DEF CON 34 we are proud to announce the new CTF organizers that will help navigate us in this new era, the **Benevolent Bureau of Birds** ! You can find the Birds online at <https://bbbirds.org/> .

The BBB joins an august lineage of CTF puzzle masters.

The People - 1996 - 2001

[Ghetto Hackers](#) - 2002-2004

[Kenshoto](#) - 2005-2008

[DDTek](#) - 2009- 2012

[Legitimate Business Syndicate](#) - 2013-2017 - <https://blog.legitbs.net>

[Order of the Overflow](#) - 2018- 2021 - <https://archive.ooo/>

[Nautilus Institute](#) - 2022-2025

Your first opportunity to sample what the Birds have in store for us will be the DC 34 CTF Qualifier Round, scheduled for May 22-24 2026.

If you're a seasoned competitor, we thank you for the part you play in this legacy. If you're new, or still thinking about it, we invite you to get yourself up to speed at the [DEF CON CTF resources page](#) . It's stocked full of recaps, walkthroughs, files and articles to show you what you can expect from our flagship contest.

We hope we'll see you in the arena.

Hotel Room Blocks for DEF CON 34 are Open!

Posted 2026-02-14

Good news, everyone!

The DEF CON 34 room blocks are live! While supplies last, you can get a special room rate at the following hotels:

Fontainebleau

Swanky, luxurious and conveniently located across the street from the LVCC. For those who must be first in line.

Sahara

Legendary Vegas spot with next-level pools and right on the monorail.

Wynn and Encore

Lovely accommodations and tons of cool places to eat and be entertained.

Circus Circus

Budget friendly and has a haunted house AND an arcade. We promise the clowns are friendly.

We're halfway there. DEF CON 34 will be upon us before you know it - be prepared and save yourself some coin.

See you soon!

DEF CON Franklin Project Hackers' Almanack released from DC33!

Posted 2026-02-12

The [DEF CON 33 Hackers' Almanack](#) translates a year of hacker research into plain language for policymakers—covering offensive AI, cybercrime, authoritarian surveillance, and critical infrastructure vulnerabilities.

This isn't a marketing report. It's a reality check.

Remaining DEF CON 34 Calls are Open!

Posted 2026-02-05

DEF CON 34 Update! All of the [calls for DC34 in Vegas are now live](#) , including the Calls for Papers, Workshops, Demo Labs, and Policy. If you're looking to participate in a creator capacity, the submission doors are open and the clock is running. Choose your adventure.

DEF CON 34 Content Calls are Open!

Posted 2026-02-02

Good news,everyone! We consulted the groundhog and [DEF CON 34 content call](#) season is officially open!

Starting today, the calls for

Villages
Contests
Communities
Parties
Meetups
Events
Music
Soundtrack
Authors
Vendors
Exhibitors
Sponsors
Press Reg

Are all ready to accept your submissions.

CFP, Workshops, Demo Labs and Policy calls will open shortly.

Let's go.

DEF CON Singapore Online Registration for Tickets and Training is Open!

Posted 2026-1-29

The wait is over. Online registration is now open for our very first DEF CON Singapore! It's all happening at the Marina Bay Sands, April 28-30. Online registration will be open until April 24, but if you secure your spot before February 15 there's an Early Bird discount available, along with a Student discount.

To learn about the speakers, contests, events, villages and other DEF CON fun we're bringing to Singapore, visit the [DEF CON Singapore site](#).

DEF CON Singapore Training registration is open as well! Join us before the conference (April 26-27) If you're looking to level up your skills with some intense, hands-on education from our world class trainers. Sessions and pricing are online at the [DEF CON Training site](#).

We're excited to bring the DEF CON experience to Singapore, and we're inspired by all the local and regional communities and talent we've brought on board to help make this a unique event.

Tickets for the conference and the trainings are waiting for you at the [DEF CON Singapore Shop](#).

See you in Singapore!

Villages, Communities, and Contests for DEF CON Singapore!

Posted 2026-1-22

Big website updates for DEF CON Singapore!

You can now find information on many of the [Villages](#), [Contests](#), and [Communities](#) you'll find when you join us in April.

We hope you'll take some time to get familiar with the lineup, and maybe even begin getting your DEF CON strategy together.

We look forward to sharing more in the coming days. See you soon!

DEF CON Singapore Trainings are Live!

Posted 2026-1-6

The DEF CON Training Singapore course lineup is now live!

We're thrilled to share the full slate of courses for the first-ever DEF CON Training Singapore! Join us in April for hands-on, skills-forward trainings led by top practitioners from across the community. Whether you're sharpening fundamentals or diving deep into emerging threats and advanced techniques, there's something here for you!

[Explore the full lineup and course details.](#)

Spots go fast, so take a look, grab your seat, and get ready to learn and build.

Early bird pricing available now until February 8. See you in Singapore

Happy New Year!

Posted 2026-1-1



Heartfelt thanks to the DEF CON community for your support in 2025. Here's hoping your 2026 exceeds your dreams.

We've got big plans for the New Year. In addition to DC34 in Las Vegas we're returning to Bahrain and adding DEF CON Singapore. New CTF runners. More trainings. We're excited and we hope you are, too.

Keep in touch with us for updates and deadlines. Look out for each other. See you soon.

DEF CON 34 Call for Trainers is Open!

Posted 2025-12-4

We're excited to announce that the [Call for Trainers is now OPEN](#) for DEF CON Training Las Vegas at DEF CON 34!

Are you passionate about cybersecurity, hacking, and hands-on learning? Do you have expertise in emerging threats, defensive strategies, or cutting-edge security techniques? We want to hear from you!

Visit training.defcon.org to submit your application by January 12, 2026.

DEF CON Singapore Calls for Papers and Demo Labs are Open!

Posted 2025-12-3

Good news, everyone! The DEF CON Singapore [Calls for Papers](#) and [Demo Labs](#) are now OPEN. If you've got a presentation or an open source project that you want to share with the DEF CON community at our first ever Singapore event, it's time to get your submission ready. The deadline is Feb 15, 2026, and it will be here before you know it. Don't delay.

We can't wait to see what you're cooking up.

DEF CON 34 and 35 Dates!

Posted 2025-10-29

Good News, Everyone! We have the official dates for DEF CON 34! And to make up for the delay, we also have the dates for DEF CON 35!

Please join us at the Las Vegas Convention Center August 6-9 in 2026 and August 5-8 in 2027.

Save the dates, friends. It'll be here before you know it.

See you there.

DEF CON Singapore Call for Creators!

Posted 2025-10-14

DEF CON Creators alert! The Call is open for Creators! Got an idea for a Contest, Village or Community you'd like to see at DEF CON Singapore? Get your submission in and let's work together to bring your ideas to life. The info you need is on the [DEF CON Singapore Call for Creators form](#) . Let's make something amazing!

DEF CON 33 Videos are Live on YouTube!

Posted 2025-10-10

Good thing there's a weekend coming up - the #defcon Youtube channel has dropped [a few hundred DEF CON 33 videos](#) for your leisurely perusal. Clear your schedule and let the dc33 Main Stage and Creator Stage Talks wash over your thirsty brain.

Even more dc33 village and music goodness on the way.

As always, enjoy and pass it on.

Call for CTF Organizers!

Posted 2025-10-09

After four excellent years, Nautilus Institute is retiring from running the official DEF CON CTF. That means the search is on for the next team to run the world's premier CTF competition. Is it your turn? Is your crew the future of live hacking competitions?

Successful applicants are:

- Fanatically dedicated.
- Radically resourceful.
- Diabolically clever.
- Disrespectful of boundaries.

Selected crew receives:

- The freedom to bring your vision to the best CTF squads on Earth.
- Glory that echoes through eternity. Your name alongside immortals like Nautilus Institute, Order of the Overflow, LegitBS, DDTEK, Ghetto Hackers and The People.
- The satisfaction that comes from knowing you raised the bar and changed the CTF game forever.
- The thanks of a grateful community.

If this sounds like you, get the details at The [DEF CON Call for CTF Organizers Page](#) , and take the first step towards your destiny. Glory awaits.

DEF CON Singapore Call for Trainers!

Posted 2025-10-07

DEF CON Training is headed to Singapore!

In April 2026, the first-ever DEF CON Singapore, co-hosted with @ HTX (Home Team Science & Technology Agency) and @ Centre for Strategic Infocomm Technologies (CSIT), will kick off with two days of world-class instruction on cutting edge topics.

Want to join us? The [Call for Trainers \(CFT\) is now open](#) and accepting applications until 11:59 pm PT on November 10.

Be sure to take a look at the list of topics of interest to provide your application the greatest chance of success.

Send submissions and questions to training@defcon.org. We hope to see you there!

DEF CON in the News!

Posted 2025-09-16

The [DEF CON Franklin project](#) got some coverage on NPR !

To learn more about Franklin's mission to connect volunteers to under-resourced infrastructure organizations, please stop by defconfranklin.com .

DEF CON Bahrain Call for Demo Labs!

Posted 2025-09-03

The Call for Demo Labs is open. If you have an open-source project, tool or technique to share with the DEF CON audience, your moment has arrived.

The submission deadline is October 5, so get your submissions in ASAP.

We've got all the info and the submission link on the [DEF CON Bahrain Page](#) .

We can't wait to see what you're working on!

Sampling of headlines from DEF CON 33

Posted 2025-08-18

Another DEF CON is in the books, and as usual we made a little news. Here's a few of the stories that came out of DEF CON 33. Watch this space for the full roundup soon.

[Wired: A Special Diamond Is the Key to a Fully Open Source Quantum Sensor](#)

[Wired: Ex-NSA Chief Paul Nakasone Has a Warning for the Tech World](#)

[ABC News: 'Hacker-volunteers' set to help water utilities with cybersecurity](#)

[NBC Chicago: Inside Defcon: What Happens at the Annual Hacker Convention](#)

[MENAFN: Phishing-Resistant Passkeys Shown To Be Phishable at DEF CON 33](#)

[CSO Online: 'Win-DDoS': Researchers unveil botnet technique exploiting Windows domain controllers](#)

[NAI500: DARPA's AI Cyber Challenge Puts CRWD, PANW, MSFT on Notice as Theori Snags \\$1.5 Million at DEF CON](#)

[Hacker News: Linux-Based Lenovo Webcams' Flaw Can Be Remotely Exploited for BadUSB Attacks](#)

[Mobileworld: Critical Zero Trust Security Flaws Exposed at DEF CON 33, Affecting Major Enterprise Vendors](#)

[Yahoo Finance: DARPA touts value of AI-powered vulnerability detection as it announces competition winners](#)

[TechCrunch: After researchers unmasked a prolific SMS scammer, a new operation has emerged in its wake](#)

Thanks for a Fantastic DEF CON

Posted 2025-08-10

DEF CON 33 is winding down now, and we want to take a moment to thank the whole DEF CON community for another amazing year. Thank you for bringing your boundless energy and curiosity to this little party we throw. Thank you for spending another long enchanted weekend teaching each other, learning from each other, and partying with each other.

It's good to spend some time with your people.

As always, if you want to keep that DEF CON feeling going all year long, consider joining a DEF CON Group. If you can't find one close to home, consider starting one. Join our Discord. Start a project you might want to share next year.

Thanks for sticking with us through the last few crazy years. Know that we're already scheming how to make next year even better.

[Return to Index](#)

© 1992-2026 DEF CON Communications, Inc. All Rights Reserved | [DEF CON Policies](#) | [DMCA Information](#)

DEF CON FAQ

Frequently asked questions about DEF CON

What is DEF CON?

DEF CON is one of the oldest continuously running hacker conventions around, and also one of the largest.

How did DEF CON start?

Originally started in 1993, it was meant to be a party for members of "Platinum Net", a Fido protocol based hacking network out of Canada. As the main U.S. hub I was helping the Platinum Net organizer (I forget his name) plan a closing party for all the member BBS systems and their users. He was going to shut down the network when his dad took a new job and had to move away. We talking about where we might hold it, when all of a sudden he left early and disappeared. I was just planning a party for a network that was shut down, except for my U.S. nodes. I decided what the hell, I'll invite the members of all the other networks my BBS (A Dark Tangent System) system was a part of including Cyber Crime International (CCI), Hit Net, Tired of Protection (ToP), and like 8 others I can't remember. Why not invite everyone on #hack? Good idea!

Where did the name come from?

The short answer is a combination of places. There was a SummerCon in the summer, a HoHoCon in the winter, a PumpCon during Halloween, etc. I didn't want any association with a time of year. If you are a Phreak, or just use your phone a lot you'll note "DEF" is #3 on the phone. If you are into military lingo DEF CON is short for "Defense Condition." Now being a fan of the movie War Games I took note that the main character, David Lightman, lived in Seattle, as I do, and chose to nuke Las Vegas with W.O.P.R. when given the chance. Well I knew I was doing a con in Vegas, so it all just sort of worked out.

There are several resources that will give you an idea of what DEF CON is all about.

[DEF CON Press](#): through the prism of the media

[DEF CON Groups](#): Local groups that meet

[DEF CON Media Server](#): DC 1 to the present, captured

[Google](#): always a good research starting point

Just remember, DEF CON is what you make of it.

When and where is DEF CON?

DEF CON is generally in the last week of July or first week of August in Las Vegas. DEF CON 34 will be held August 6th through August 9th, 2026. Many people arrive a day early, and many stay a day later.

Isn't there a DEF CON FAQ already?

Yes, an unofficial one. It's quite humorous, sometimes informative, and DEF CON takes no responsibility for its content. It is archived [here](#).

What are the rules of DEF CON?

Physical violence is prohibited. Harassment of any kind is prohibited. We don't support illegal drug use. Minors should be accompanied by their parent(s) or guardian(s). Please refrain from doing anything that might jeopardize the conference or attendees such as lighting your hair on fire or throwing lit road flares in elevators. DEF CON Goons are there to answer your questions and keep everything moving. Hotel security is there to watch over their property. Each has a different mission, and it is wise to not anger the hotel people. Please be aware that if you engage in illegal activities there is a large contingency of feds that attend DEF CON. Talking about how you are going to bomb the RNC convention in front of an FBI agent is a Career Limiting Move!

You can view the DEF CON Code of Conduct at <https://defcon.org/html/links/dc-code-of-conduct.html>.

Is DEF CON cancelled?

No.

What is there to do at DEF CON?

DEF CON is a unique experience for each con-goer. If you google around you'll find dozens of write-ups that will give you an idea of what people have experienced at DEF CON. Trust write-ups more than media articles about the con. Some people play capture the flag 24x7, while many people never touch a computer at DEF CON. Some people see every speech they can, while others miss all speeches. Other activities include contests, movie marathons, scavenger hunts, sleep deprivation, lock picking, warez trading, drunken parties, spot the fed contest, the official music events. Because DEF CON is what the attendees make of it, there are more events than even we are aware of. Half the fun is learning what happened at DEF CON after the fact!

I'm not a hacker, should I go to DEF CON?

Many people have different definitions of what is a 'hacker'. I would recommend looking at previous years speeches, and write-ups from past attendees - this should give you a good idea if DEF CON is for you. This hacker FAQ might give you some insight into the matter as well. If you do not have any technical interests, DEF CON is probably not for you. Sure there is a lot of socializing you can do, but technology and hacking is the core of the con.

Do criminals go to DEF CON?

Yes. They also go to high school, college, work in your workplace, and the government. There are also lawyers, law enforcement agents, civil libertarians, cryptographers, and hackers in attendance. Ssshhh. Don't tell anyone.

What are Goons?

They are the staff at DEF CON. They have many roles including safety, speaker coordination, vendor room coordination, network operations, et cetera... Please try to be helpful to them if they make requests of you. If any goon tells you to move, please do so immediately as there may be safety issues they are attempting to address.

How can I help out or become a Goon?

The staff at DEF CON has grown organically. All positions have some degree of trust associated with them, so typically new goons are 'inducted' by friends of existing goons. There are many random points when goons need help and may ask people for help, generally for helping move stuff or other tasks that don't require high amounts of trust or unsupervised work. Just because you help out doesn't make you a goon. If you really want to be a goon, talk with one and see how much work they actually do (Hint: you may want to enjoy being at DEF CON, not working full-time at it). One year the network group got a new Goon when a networking engineer was needed, and he came to the rescue. The intent behind the goons is not to be elitist, but to have a network of trusted people who can help run the conference - please do not feel upset if you are not chosen to be a goon.

How can I help or participate?

DEF CON is not a spectator sport! Before the con, during, and after there are chances for you to get involved. Before the con you can read about the contests and maybe sign up for one like Capture the Flag. There are artwork contests for shirts and posters. You can practice your lock pick skills, or just get your laptop all locked down and ready to do battle. Organize your .mp3s. Check out the DEF CON Forums to see what other people are up to. If you want to create your own event, you can do that as well - you will not get official space or sanctions, but virtually every official event at DEF CON started out as an unofficial event.

I would love to see XYZ event, how do I make this happen?

Virtually all events at DEF CON were conceived by the attendees. The DEF CON forums are a great place for recruiting help for an event you want to put on, and making sure your efforts aren't being duplicated. If it doesn't require resources from DEF CON (space, namely) you generally don't have to ask anyone's permission. Most events are unofficial until they've been going on for a couple of years. Please let us know if you have an idea for an event, we may help facilitate or promote it. Email [suggestions at DEF CON dot org] to keep us in the loop.

How can I speak at DEF CON?

You can submit a response to our CFP (opening soon). All entries are read and evaluated by a selection committee. We would love to have your submission. The call for papers usually opens in January and closes mid-May.

I'm press, how do I sign up, why can't I get in for free (I'm just doing my job)?

Please email press@defcon.org if you wish press credentials. Lots of people come to DEF CON and are doing their job; security professionals, federal agents, and the press. It wouldn't be fair to DEF CON attendees if we exempted one group from paying. If you are a major network and plan on doing a two minute piece showing all the people with blue hair, you probably shouldn't bother applying for a press pass - you won't get one. If you are a security writer or from a real publication please submit, and someone will respond with an answer.

I want to sell stuff, how do I do this?

If you want a space in our vendor area, you need to apply. Because of limited space and our attempt to have a diversity of vendors, you may not be able to get a booth. It is wise to think of staffing issues - if you are one person do you want to spend your entire time behind a vendors booth?

What are the different price rates?

Everyone pays the same: The government, the media, the 'well known hackers', the unknown script kiddies. The only discount is for Goons and speakers, who get to work without paying for the privilege.

Does my underage child need a badge?

Children under the age of 8 will not need to purchase a badge.

Can I get a discount on DEF CON badges?

DEF CON charges one price regardless of your social status or affiliation. Please know that we depend on attendee income to pay the costs of the conference and don't have sponsors to help defray the expenses.

We sometimes get requests for discounts [students, veterans, children], unfortunately we don't want to try and validate if you are a current student, look at your ID to determine your age, decode military discharge papers, etc.

If you really want to attend DEF CON for free then do something for the con.

You could:

Submit a CFP and be an accepted speaker or workshop instructor.

Work on a contest, event, or village.

Qualify for CTF/Contests that include entry.

Find a team to become a Goon newbie.

Contribute to content, or perform some entertainment.

I need a letter of invite for my visa application, how do I get that?

In most cases, DEF CON can send a signed letter of invite, usually within a few short business days once we have all the info. If you also require verification of housing, we can put you in touch with someone to help you get your hotel stay organized, let us know if you need that.

To request an invitation letter, fill out this form: <https://wkf.ms/3Z9hMF4> Once approved, your invitation letter will be emailed to you.

DEF CON is too expensive, how can I afford it?

Many people have made an art and science out of coming to DEF CON very cheaply. Here are a couple of tips.

Travel: Buy airfare in advance, go Greyhound, Carpool, hitch-hike. (Note: this may be dangerous and/or illegal.)

Lodging: Share rooms - some people have up to 10 people they share a room with, find a hotel cheaper than the one that the conference is scheduled at, stay up for three days, etc. (note: this can be hazardous to your health.)

Food: Pack food for your trip, go off site to find food, eat in your hotel rooms, and look for cheap Vegas food at Casinos. (Look for deals and specials that are trying to get you in the door to gamble.)

Booze: You don't need to drink. Brew your own and bring it. (It's been done.)

Entrance: Admission can be saved, mow some lawns. Try to go to another 4 day event for cheaper than this that offers so much. We have increased the fees slowly over the years, but also the amount and quality of events have increased.

Inevitably people will try to do some math and pretend that DT gets rich each DEF CON - they seem to lack the ability to subtract.

How many people typically attend DEF CON?

There have been roughly 25-28k attendees in the last few (pre-COVID) years of DEF CON. DEF CON 27 had a record showing with approximately 30,000.

Is there a network at DEF CON?

Why yes, DEF CON is FULLY network-enabled. Now that we've perfected the art of a stable hacker con network, we're ascending to a higher level - we're providing you a network that you feel SAFE in using! Since DEF CON 18 we're WPA2 encrypted over-the-air, with a direct trunk out to the Internet. No peer-to-peer, no sniffing, just straight to the net (and internal servers). We'll provide login credentials at Registration. We know the LTE airwaves will be saturated so we're putting our own cred on the line to give you a net that even we would put our own mobile phones on.

If you're feeling frisky, we'll still have the traditional "open" network for you - bring your laptop (we'd recommend a clean OS, fully patched--you know the procedure) because we don't police what happens on that net. Share & enjoy!

What is the age limit?

People have brought children to DEF CON - it is not recommended to do this unless you are going to constantly supervise them. It is generally an 'adult' atmosphere (language, booze, et cetera). If you've never been to DEF CON, you may want to refrain from bringing your children (unless they are demanding that you bring them). While there are no age limits, we have consistently cooperated with parents and/or private investigators who are looking for children that 'ran away from home' to go to DEF CON. You will have to be 21 to reserve a room.

What is a DEF CON "Black Badge"?

The Black Badge is the highest award DEF CON gives to contest winners of certain events. CTF winners sometimes earn these, as well as Hacker Jeopardy winners. The contests that are awarded Black Badges vary from year to year, and a Black Badge allows free entrance to DEF CON for life, potentially a value of thousands of dollars.

How can I get a hold of DT? I tried to mail him and haven't seen a response yet.

DT doesn't dislike you, isn't trying to hurt your feelings, and bears you no ill will. The fact is he gets an unmanageable load of mail continually. Mailing him again may elicit a response. Try mailing FAQ (at) DEFCON.ORG if you have a general question that isn't answered here or in the forums.

Is it hot in Vegas?

Yes. Bring sunscreen (high SPF), do not fall asleep near the pool (lest you wake up to sunburn), and do not walk far in the sun unless you are experienced in dealing with extreme heat. The sun is dangerous in Las Vegas. Sleeping in lawn chairs is a sure way to wake up to severe burns in the morning when that bright yellow thing scorches your skin. Drink plenty of water and liquids - remember that alcohol will dehydrate you.

What should I bring?

It depends on what you're going to do at DEF CON. This is discussed in quite some depth on the [unofficial DC FAQ](#), as well as a thread in the DC Forums. You may want to bring fancy (or outrageously silly) clothes for the official Music events, on Friday and Saturday nights, where everyone shows off nifty attire.

How much do rooms cost, and how do I reserve a room?

Room Block info can be found on the home page of defcon.org

How much is internet access?

We are looking into this. Free (and possibly more dangerous) internet access is available in the convention area.

Will the hotels broadcast the speeches on their cable system?

DEF CON TV has successfully streamed all tracks to all the hotels in the past, and a couple of tracks out to the internet, for several years now. We have been streaming on twitch the last couple of years

Will we have DEF CON branded poker chips?

You will have to attend DEF CON to find out.

Will conference attendees have entire floors of hotel rooms to themselves?

Probably not. Hotels have been very cooperative in attempting to centralize the DEF CON attendees, for their convenience and ours, but there will be non-DEF CON attendees in hotel rooms next to us.

This FAQ didn't answer my questions, or was unclear, how can I get further information?

Check out the [DEF CON Forums](#) to ask follow up questions.

DEF CON Villages Table

Each Village, as it's name may imply, specializes in a topic or aspect of security or computers.

One Page [All Villages](#) list with descriptions

defcon.org [Villages](#) page

You may need to scroll to the right to see all info

Village Name Home Page	Map	Schedule	Village Desc	Social Media Links
.EDU Community	Map			
Adversary Village	Map	Sched	Desc	TW @AdversaryVillag https://defcon.social/@AdversaryVillage YT https://youtube.com/AdversaryVillage DC https://discord.gg/GDB3rC7KYz TI @AdversaryVillage FB @AdversaryVillage LI @adversaryvillage
Aerospace Village	Map	Sched	Desc	TW @secureaerospace LI @aerospace-village TW @hack_a_sat DC https://discord.gg/gV4EWuk YT https://www.youtube.com/c/AerospaceVillage https://defcon.social/@aerospacevillage
AI Village	Map		Desc	TW @aivillage_dc TI @aivillage YT link DC https://discord.com/invite/GX5fhfT LI @aivillage
AppSec Village	Map	Sched	Desc	TW @AppSec_Village LI @appsecvillage YT https://www.youtube.com/c/AppSecVillage DC https://discord.gg/5XY8qYXd7R
Badgelife Village	Map	Sched	Desc	https://reanimationxp.bsky.social/ https://github.com/badgelife/website DC https://discord.gg/R4jGhTqJ3J
Biohacking Village	Map	Sched	Desc	TW @dc_bhv LI @biohacking-village YT http://youtube.com/biohackingvillage TI @biohackingvillage DC https://discord.gg/Q8ubDb5 https://bsky.app/profile/villageb.io link
Blacks In Cyber Village	Map	Sched	Desc	TW @BlackInCyberCo1 https://defcon.social/@blacksincyber TI @blacksincybersecurity YT link LI @blackincyberconference PT @blacksincybersecurity FB @blackincyberconf

Village Name Home Page	Map	Schedule	Village Desc	Social Media Links
Blue Team Village	Map	Sched	Desc	TW @BlueTeamVillage TI @blueteamvillage YT https://www.youtube.com/c/blueteamvillage DC https://discord.gg/blueteamvillage https://defcon.social/@blueteamvillage
Bug Bounty Village	Map	Sched	Desc	TW @BugBountyDEFCON YT https://www.youtube.com/BountyTalks TW @arl_rose TW @infinetologins YT https://www.youtube.com/infinetologins IG @bugbountydefcon
Call Center Village	Map	Sched	Desc	https://defcon.social/@callcentervillage https://github.com/callcentervillage
Car Hacking Village	Map	Sched	Desc	TW @CarHackVillage YT http://youtube.com/@carhackingvillage LI @car-hacking-village DC https://discord.gg/zz7xUPZcre https://github.com/car-hacking-village
Cloud Village	Map	Sched	Desc	TW @cloudvillage_dc YT https://www.youtube.com/cloudvillage_dc DC https://discord.com/invite/p3S3KVD2Tp LI @cloudvillage-dc FB @1DVeGSw5KT IG @cloudvillage_dc
CodeBloom	Map	https://mastodon.social/@codebloom https://bsky.app/profile/codebloom.bsky.social IG @codebloomhq FB @profile.php?id=61584968176159		
Contests				link
Crypto & Privacy Village	Map	Sched	Desc	TW @cryptovillage SL https://cryptovillage.slack.com/ YT link TI @cryptovillage https://defcon.social/@cryptovillage
Cryptocurrency Village	Map	Sched	Desc	
Data Duplication Village	Map	Sched	Desc	TW @DDV_DC
DCNextGen	Map	https://defcon.social/@defconnextgen		
DEF CON Groups	Map			
DEF CON Talks				TW @defcon FB @defcon YT https://www.youtube.com/user/DEFCONConference http://www.reddit.com/r/defcon IG @wearedefcon DC https://discord.gg/defcon
DEF CON Training				
DEF CON Workshops				
Demo Labs				
Embedded Systems Village	Map		Desc	TW @EmbeddedVillage

Village Name Home Page	Map	Schedule	Village Desc	Social Media Links
Game Hacking Village	Map		Desc	YT https://youtube.com/@gamehackingvillage TW @GameHackingGG IG @gamehacking.gg DC https://discord.com/invite/bNYz8Xws8j
Hackers.town	Map			
Ham Radio Village	Map	Sched	Desc	TW @HamRadioVillage TI @HamRadioVillage DC https://discord.gg/hrv https://defcon.social/@HamRadioVillage
Hardware Hacking Soldering Skills Village (HHV-SSV)	Map	Sched	Desc	TW @DC_HHV https://defcon.social/@DC_HHV
ICS Village	Map	Sched	Desc	TW @ICS_Village LI @icsvillage YT link TI @ics_village
IoT Village	Map	Sched	Desc	TW @iotvillage TW @ISEsecurity TW @Villageidiotlab https://defcon.social/@IoTVillage/ TI @iotvillage YT https://www.youtube.com/c/IoTVillage/videos DC https://discord.gg/EFKbNFrFaN
La Villa Community	Map			TW @lavillahacker LI @la-villa-hacker IG @lavillahacker
LockPick Village	Map		Desc	TW @toool TI @toool_us YT https://youtube.com/c/TOOOL-US https://techhub.social/@TOOOL DC https://discord.gg/KVzJ9QK2az
Lonely Hackers Club	Map			https://lonelyhackers.club/telegram/ TW @L0nelyH4ckers https://defcon.social/@L0nelyH4ckers
Maker's Village	Map	Sched	Desc	DC https://discord.gg/VBwjCCvqG
Malware Village	Map		Desc	TW @MalwareVillage LI @malwarevillage DC https://discord.com/invite/xQwqY48SrJ
Maritime Hacking Village	Map	Sched	Desc	TW @maritimevillage LI @maritimehackingvillage
Middle Easterns & Africans in Cyber Security (MEACS)	Map			
Misc				
Mobile Hacking Community	Map	Sched		DC https://discord.gg/dHW7PVSCzY https://mastodon.social/@mobilehackingcommunity
Nix Vegas Community	Map			TW @NixVegas https://bsky.app/profile/nixvegas.bsky.social https://github.com/NixVegas YT https://www.youtube.com/@NixVegasDEFCON https://live.nix.vegas/

Village Name Home Page	Map	Schedule	Village Desc	Social Media Links
Noob Community	Map			https://infosec.exchange/@tracelabs TW @TraceLabs YT https://www.youtube.com/c/TraceLabsVideos LI @tracelabs https://github.com/tracelabs
OSINT For Good Community	Map			
OWASP Foundation	Map			https://infosec.exchange/@owasp YT https://www.youtube.com/user/OWASPGLOBAL TW @owasp FB @OWASPFoundation LI @owasp SL https://owasp.org/slack/invite https://github.com/OWASP/
Packet Hacking Village	Map	Sched	Desc	TW @wallofsheep FB @wallofsheep YT https://youtube.com/wallofsheep TI @wallofsheep PS https://www.periscope.tv/wallofsheep https://defcon.social/@wallofsheep IG @wallofsheep
Payment Village	Map		Desc	TW @paymentvillage TI @paymentvillage YT https://www.youtube.com/c/PaymentVillage https://t.me/paymentvillage LI @payment-village link
Physical Security Village	Map		Desc	TW @physsec TI @bypassvillage LI @physsec https://defcon.social/@physsec DC https://discord.gg/XmuEF62eun IG @physsecvillage
Policy @ DEF CON	Map	Sched	Desc	TW @DEFCONPolicy link https://defcon.social/@defconpolicy link LI @policy-def-con YT https://www.youtube.com/@policyatdefcon
Quantum Village	Map		Desc	TW @quantum_village DC https://discord.gg/6WUjH5cBXu LI @quantumvillage YT https://youtube.com/@quantum_village/
Queercon Community	Map			https://bsky.app/profile/queercon.org DC https://queercon.org/discord
Radio Frequency Village	Map		Desc	TW @rfhackers TW @rf_ctf link DC https://discordapp.com/invite/JjPQhKy
Recon Village	Map	Sched	Desc	TW @ReconVillage FB @reconvillage

Village Name Home Page	Map	Schedule	Village Desc	Social Media Links
				YT https://www.youtube.com/reconvillage/ https://www.threads.com/@recon_villa LI @reconvillage DC https://discord.gg/reconvillage
Red Team Village	Map	Sched	Desc	TW @redteamvillage_ YT https://www.youtube.com/redteamvillage TI @redteamvillage DC https://discord.gg/redteamvillage IG @theredteamvillage link
Scambait Village	Map		Desc	
Social Engineering Community Village	Map	Sched	Desc	TW @sec_defcon YT link TI @se_community LI @social-engineering-community FB @Social-Engineering-Community-108883855139272
Social Gatherings/Events				
Tamper Evident Village	Map		Desc	
Telecom Village	Map		Desc	TW @TelecomVillage LI @telecom-village
The Diana Initiative	Map			https://defcon.social/@DianaInitiative FB @dianainitiative TW @DianaInitiative link YT link IG @dianainitiative
Voting Village	Map		Desc	TW @votingvillagedc YT https://youtube.com/@defconvotingvillage TI @votingvillagedc LI @election-integrity-foundation IG @votingvillage?igsh=MWJreTh6dG13eDEzNg==

[Return to Index](#)

DEF CON Contests Table

Various contests, some lasting all 4 days of DEF CON, some short time on stage

One Page [All Contests](#) list with descriptions

defcon.org [Contests](#) page

You may need to scroll to the right to see all info

?Cube Contest Info	\$\$\$\$\$_<CAPTURE_THE_COIN>_\$\$\$\$ Contest Info
\$unL1ght Sh4d0w5 Contest Info	5N4CK3Y Contest Info
Adversary Wars CTF Contest Info	AI Art Battle Contest Info
AI Village Plays Pokemon: DEF CON Edition Contest Info	Apex Park (Cloud Village CTF) Contest Info
Aw, man...pages! Contest Info	BadgeLife Trivia Contest Info
Battle of the Bots: Vishing Edition Contest Info	Beer Chilling Contraption Contest Contest Info
Blacks In Cybersecurity Game Night Extravaganza! Contest Info	Blacks In Cybersecurity Village Capture The Flag Competition Contest Info
Blue Team Village CTF – Project Obsidian Contest Info	Bug Bounty Village CTF Contest Info
Can it Ham? Contest Info	Capture The Packet Contest Info
Car Hacking Village Capture the Flag (CTF) Contest Info	CMD+CTRL Cyber Range Contest Info
Code Cadaver (Biohacking Village CTF) Contest Info	Crack Me If You Can 2026 Contest Info
Crack the Core Contest Info	Crash and Compile Contest Info
Creative Writing Short Story Contest Contest Info	Cryptid Hunt Contest Info
Cryptocurrency Challenge Contest Info	Cyber Deck Makers' Contest Contest Info
Darknet-NG Contest Info	DC's Next Top Threat Model Contest Info
DDoS CTF – PWN UR H0M3 Contest Info	DEF CON Beard and Mustache Contest Contest Info
DEF CON CTF: Benevolent Bureau of Birds Contest Info	DEF CON Groups Backdoor & Breaches Contest Info
DEF CON Groups Sticker Contest Contest Info	DEF CON MUD Contest Info
DEF CON Scavenger Hunt Contest Info	Dozier Drill Lockpicking Challenge Contest Info

EFF Tech Trivia Contest Info	Escalation Desk CTF Contest Info
Feet Feud (Hacker Family Feud) Contest Info	Fix the Flag – The AppSec Village Wargame Contest Info
From the Static: A HRV Fox Hunt Contest Info	Game Hacking Village CTF Contest Info
Global OSINT Search Party CTF – DEF CON 34 Edition Contest Info	Hac-Man Contest Info
Hack3r Runw@y v8.0 Contest Info	Hacker Games Contest Info
Hacker Jeopardy! Contest Info	HackFortress Contest Info
Hacking GRC Contest Info	HALctf (AI Village CTF) Contest Info
Hardware Hacking Village CTF Contest Info	HardWired Contest Info
HSPACE: AI Battlegrounds Contest Info	HTB CTF: Data Dystopia Contest Info
IoT Village CTF Contest Info	Kubernetes CTF Contest Info
Locktopus Competition Contest Info	Octopus Game 5: Revenge Of The Squid Contest Info
OWASP Foundation CTF Contest Info	Phish Stories Contest Info
PhreakMe Contest Info	Pinball High Score Contest Contest Info
Pub Quiz at DEF CON Contest Info	Radio Frequency Capture the Flag Contest Info
Raitlin's Challenge presented by the Illuminati Party® Contest Info	Real7y Overrun Contest Info
Red Team CTF Contest Info	Social Engineering Community Vishing Competition (SECVC) Contest Info
spyVspy 3: Rat Race Contest Info	STARPWN (Aerospace Village CTF) Contest Info
TeleChallenge Contest Info	The EFF Benefit Poker Tournament Contest Info
The Gold Bug (Crypto and Privacy Village Contest) Contest Info	The Pwnie Awards Contest Info
Tin Foil Hat Contest Contest Info	Um, ACKtually Contest Info
Untechnical Contest Info	Venator Aurum Contest Info
Whose Slide Is It Anyway? Contest Info	

[Return to Index](#)

DEF CON DemoLabs Table

Brief demonstrations for people to show off their project.

One Page [All Demolabs](#) list with descriptions

defcon.org [DemoLabs](#) page

You may need to scroll to the right to see all info

AC Scanner: The Post-Quantum Cryptographic Exposure and CBOM Generator. You Need This! Demolabs Info
AD-Necromancer: Resurrecting Forgotten Control Paths in Active Directory Demolabs Info
AI Pipeline for N-days Weaponization Demolabs Info
AOBTD: AI One Bites The DAST Demolabs Info
AzProwl: Prowling the Azure Attack Surface Demolabs Info
Be like a BRAT(BLE Recon and Attack Toolkit): Skip the Handshake, Own the Device Demolabs Info
Beyond Spidering: Behavior Driven DAST for Real Application Workflows Demolabs Info
BigIron.ai: AI-Assisted Exploration and Security Analysis of Mainframe Systems Demolabs Info
Clew: Untangling Evasive Malware with Per-Sample Fuzzing Seeds Demolabs Info
Damn Vulnerable Agentic AI Application (DVAIA) Demolabs Info
DFMI: Weaponizing MSI Installers for Fileless Code Execution Demolabs Info
Empire 7: Shipping a C2 at AI Speed Demolabs Info
Ghost in the IDE Demolabs Info
GhostCatcher (endpoint detection agent) Demolabs Info
GnawLab: Open-Source AWS Attack Scenarios Based on Real-World Breaches Demolabs Info
Goose Processing Unit (GPU): VRAM as an Unmonitored Attack Surface Demolabs Info
Hook Crook – Extracting More From Discord Webhooks Demolabs Info
Intercept.js: Runtime-Aware Detection for JavaScript Environments Demolabs Info
Keychecker : SSH Key based attack tool for DVCS Systems Demolabs Info

L.A.Y.E.R.S – Layered Analysis Engine for Browser Extension Risk and Security Demolabs Info
LoKi: A LoRa/Meshtastic based implant for Red Teaming Demolabs Info
MailX-Ray: A TSA X-Ray for Emails — Air-Gapped Safe-Read and Quick Triage in an Ephemeral MicroVM Demolabs Info
MalSkill Lab: Hands-On Natural Language Malware in AI Agent Orchestration Systems Demolabs Info
Monitor, Compile, Enforce: A Compiler Pipeline for Container Security Policy in Rust and eBPF Demolabs Info
MSCodePhish: Redeem Your Coupon. Surrender Your Session Demolabs Info
Overcast: Video OSINT Agent. Point It at 100 Videos, Ask Anything Demolabs Info
Peekaboo: Breaking the Black Box of Threat and Malware Emulation Demolabs Info
Phasmid: Deniable Storage for Rubber-Hose Scenarios Demolabs Info
PromptPwn: Finding and Exploiting AI-Generated Vulnerabilities at Scale Demolabs Info
pymsi: Interactive MSI Installer Analysis in Python and the Browser Demolabs Info
Reversing F5: Pure-Go Steganography, Live Forensic Cover Recovery, and JPEG Fragility Analysis Demolabs Info
SecretSifter: Production Apps Are Leaking Credentials. The Blindspot DAST Never Checked. Demolabs Info
Senrigan () x Suzaku (): Threat Hunting & DFIR for AWS — No SIEM, Just Your Laptop Demolabs Info
sisakulint:CI-Friendly static linter with autofix, SAST, semantic analysis for GitHub Actions Demolabs Info
TokenMesh: Exposing Azure’s Hidden Identity Attack Surface Demolabs Info
Trajan: Cross-Platform CI/CD Security Scanner Demolabs Info
VoiceLock: Offline, Robust On-Device Speech Transcription Demolabs Info
Weaponizing eBPF and XDP with Covert Triggered Reverse Shells Demolabs Info
X-Ray Your Agents: Pentesting MCPs, Skills, and the Plugin Supply Chain Demolabs Info
xEndity: IoT Firmware Analysis & Digital Twin Platform Demolabs Info
Zealot: An Autonomous Cloud Offensive Multi-Agent System Demolabs Info
Zero-Cloud Threat Modeling: Vector Embedding Architectures for Automated Vulnerability Detection Demolabs Info

[Return to Index](#)

DEF CON Workshops Table

Longer, more detailed, hands on, lasting half a day.
These have limited seating. These will fill up VERY quickly!

One Page [All Workshops](#) list with descriptions

defcon.org [Workshops](#) page

You may need to scroll to the right to see all info

Sold Out – Agentic Threat Hunting: Building AI That Remembers What You Hunted DC Workshop Info
Sold Out – All About Stoopie InfoStealers: Malware Analysis for Understanding, Custom Coding for True Understanding! DC Workshop Info
Sold Out – Attacking Cloud APIs from the IoT Edge DC Workshop Info
Sold Out – AWS Cloud Security 101: From IAM Misconfigurations to Account Takeover DC Workshop Info
Sold Out – AWS Principal Threat Hunting: Behavioral Baselining for Malicious Activity DC Workshop Info
Sold Out – Battle-Tested Broadcasts: RF Insights From Ukraine DC Workshop Info
Sold Out – Building Agentic Reverse Engineering “Skills” DC Workshop Info
Sold Out – Building your own hardware hacking kit to Pentest Bluetooth, WIFI, and more. DC Workshop Info
Sold Out – CI/CD Weaponization: Build It, Deploy It, Own It DC Workshop Info
Sold Out – Creating Shellcode for Hackers DC Workshop Info
Sold Out – Detecting and Analyzing Memory Only Malware with Volatility 3 DC Workshop Info
Sold Out – Embedded Computing Tools for Wireless Hardware Hacking DC Workshop Info
Sold Out – Entra ID Persistence – Because Passwords Were Never the Problem DC Workshop Info
Sold Out – Explore the Windows instrumentation callback DC Workshop Info
Sold Out – From Prompt to PWN: Exploiting LLM Powered Web Applications with OWASP Techniques DC Workshop Info
Sold Out – HackTheCloud26: Chaining Cloud Misconfigurations to Compromise Infrastructure DC Workshop Info
Sold Out – Hands-on DuckyScript: An Introduction to HID Attack Tools with O.MG Devices DC Workshop Info
Sold Out – Hands-on IoT firmware extraction and flash forensics DC Workshop Info
Sold Out – Hecate: A Trivial UART Tool DC Workshop Info

Sold Out – ICS Hack ‘n Track DC Workshop Info
Sold Out – Intro to Writing Windows Malware with Rust! DC Workshop Info
Sold Out – Introduction to Malware Analysis DC Workshop Info
Sold Out – Investigating and Responding to M365 account compromise on a shoestring: Living of the Land Incident Response DC Workshop Info
Sold Out – Learning to Hack Bluetooth Low Energy with BLE CTF DC Workshop Info
Sold Out – Learning to Reverse Engineer Compiled C as We Learn to Write It DC Workshop Info
Sold Out – Long Live Empire: A C2 Workshop for Modern Red Teaming DC Workshop Info
Sold Out – Malware Development 101 – From Zero to Hero: Adapt your payload to your environment DC Workshop Info
Sold Out – Offensive Packet Wizardry with Scapy DC Workshop Info
Sold Out – OT Systems: how to secure them in practice! DC Workshop Info
Sold Out – Pivot, Hunt, Publish: An Offline, Hands-On CTI Workshop for Blue Teams and Threat Researchers DC Workshop Info
Sold Out – Post-Quantum Cryptography (PQC) for Hackers DC Workshop Info
Sold Out – Purple Protocol: Adversary emulation for everyone DC Workshop Info
Sold Out – Purple Teaming Industrial Control Systems DC Workshop Info
Sold Out – Reaching Mythos: Hands-On Vulnerability Discovery with Local AI Models DC Workshop Info
Sold Out – Salesforce Apex Predator: Breaking Salesforce Sites DC Workshop Info
Sold Out – Solder, Detect, Listen: Build Your Own EMF Explorer DC Workshop Info
Sold Out – Step-by-Step Malware Development: Evading EDR from Loaders to the Kernel DC Workshop Info
Sold Out – Web Hacking 101 DC Workshop Info
Sold Out – Wi-Fight Club: I am Jack’s Evil Twin DC Workshop Info
Sold Out – Words As Weapons: Breaking AI and Agents; Then Securing Them DC Workshop Info

[Return to Index](#)

DC Paid Training Table

2 day training sessions on the Mon and Tue after DEF CON. There will be an additional cost for these.

One Page [All Paid Training](#) list with descriptions

DEF CON 34 Training [Signup Pages](#)

You may need to scroll to the right to see all info

Advanced Cloud Incident Response in Azure and Microsoft 365 Training Info
Advanced Windows Binary Exploitation Training Info
Adversarial Thinking: The Art of Dangerous Ideas Training Info
Agentic AppSec: Harnessing LLMs Training Info
Agentic RE: Automating Reverse Engineering & Vulnerability Research with AI Training Info
AI + SOC 101 Bootcamp: Building Modern Security Operation Skills with AI Integration Training Info
AI Agent Security Masterclass: Attacking and Defending Autonomous AI Systems Training Info
AI SecureOps: Attacking & Defending AI Applications & Agents Training Info
Analyze, Detect & Hunt: Hands-On Malware Analysis, Memory Forensics & AI-Driven Threat Hunting with Endpoint Telemetry Training Info
Applied SDR Hacking: Red Team SIGINT for mission-critical, automotive, aviation, and marine targets Training Info
Beat the Breach: Defend, Respond, Survive Training Info
Black Belt Pentesting / Bug Hunting Millionaire: Mastering Web Attacks with Full-Stack Exploitation (100% Hands-On) Training Info
Blue vs Red Bootcamp: From Attacker Playbooks to Defender Detections Training Info
Breaking Physical Access Control: Electrical Fundamentals, RFID Credentials, and Hands-On Offense Training Info
Breaking the Cloud Layer – Modern and Practical Attacks on AWS, Azure, GCP, Aliyun, Railway and Vercel Training Info
Bridging the GAP: Hands-On Embedded Hardware Hacking Training Info
Car Hacking Masterclass – Attacking & Defending Automotive Systems and Infrastructure Training Info
Cyber & AI Policy Basics: What Every Organization Needs in Place Training Info
Dark Wolf Hack Our Drone Workshop Training Info

Deep Dive into the Dark Web Training Info
Digital Supply Chain Security: Software, Cryptography, AI, and Vendor Risk Training Info
Full-Stack Pentesting Laboratory: 100% Hands-On + Lifetime LAB Access Training Info
Hacking Android and IOT Apps by Example Training Info
Hacking Cryptography Training Info
Influence Operations: Tactics, Defense, and Exploitation Training Info
IoT Exploitation Masterclass: Hardware & RF Hacking Training Info
Offensive Cyber Security Operations: Mastering Breach and Adversarial Attack Simulation Engagements Training Info
Securing the Future: Defending Kubernetes & Cloud-Native Infrastructure in the Age of AI Training Info
Simulated Adversary: Tactics & Tools Training Training Info
Software Defined Radios 101 – Introduction to RF Hacking Training Info
Solving Modern Cybersecurity Problems with AI Training Info
Strategic AI Penetration: Mastering Offensive Techniques for LLMs Training Info
VS: S-RAD (Satellite-Radio Analysis & Disruption) Training Info

[Return to Index](#)

DC Party,Gather,Event Table

Various Parties, Gatherings, and Events

One Page [All Parties, Gatherings, Events](#) list with descriptions

defcon.org [Parties, Meetups, and Events](#) page

You may need to scroll to the right to see all info

+61: the Australian Embassy Event Info	10 years of K-rad (Hackers.Town Party) Event Info
15th Cycleoverride Bike Ride at DEF CON Event Info	2nd Annual Spades Night & Uno Tournament Event Info
Arcade Party Event Info	Atlanta Metro Meetup (DC404/DC678/DC770/DC470) Event Info
BIC R00T ACCESS 2026 Event Info	BlanketFort Con Event Info
Blue Team Village Movie Night Event Info	Book Signing – Aamiruddin Syed Event Info
Book Signing – Avinash Majeti Event Info	Book Signing – Brandy Smith Event Info
Book Signing – Christopher DeCarmen Event Info	Book Signing – Cindy Cohn Event Info
Book Signing – Garrett Gee Event Info	Book Signing – Laura Scherling Event Info
Book Signing – Mark Foudy Event Info	Book Signing – Michael Robinson Event Info
Book Signing – Nicholas DeMeo Event Info	Book Signing – Ted Harrington Event Info
Book Signing – Thomas Wilhelm Event Info	Conference Planners Meetup Event Info
Day of the Dead Hacker Party Event Info	DC702 Meetup Event Info
DC713 and DC281 – 8th Annual DEF CON Texas Groups Meetup Event Info	DCG New England Meetup Event Info
DCNextGen Party! Event Info	DEF CON After party @ LIV Fontainebleau Event Info
Defcon.run Event Info	Exploit Your Own Story Event Info
Free Ham Radio License Exams Event Info	Friends of Bill W Event Info
Front Man’s Fête: An Octopus Game Party (including Octopus Game winners and prizes) Event Info	GOTHCON Event Info
Hacker Book Club Discussion Event Info	Hacker Jeopardy Event Info
Hacker Karaoke Event Info	Ham In A Day Class Event Info

Human Registration Open Event Info	Illuminati Party Event Info
Kayos Klub Event Info	Lawyers Meet Event Info
Linecon Event Info	Malysis: A Bare-Metal RAM Enclave for Malware Analysis. No Hypervisor. No Trace. Event Info
Malysis: A Bare-Metal RAM Enclave for Malware Analysis. No Hypervisor. No Trace. Event Info	Merch (formerly swag) Area Open — README Event Info
Movie Night Event Info	Music – Genre: Breakbeats Event Info
Music – Genre: Breakbeats Event Info	Music – Genre: Drum & Bass Event Info
Music – Genre: Drum & Bass Event Info	Music – Genre: Drum & Bass Event Info
Music – Genre: Drum & Bass Event Info	Music – Genre: Dubstep Event Info
Music – Genre: Electro House Event Info	Music – Genre: Goth / Industrial Event Info
Music – Genre: Goth / Industrial Event Info	Music – Genre: House Event Info
Music – Genre: House Event Info	Music – Genre: Nerdcore Event Info
Music – Genre: Nerdcore Event Info	Music – Genre: Techno Event Info
Music – Genre: Techno Event Info	Music – Genre: Techno Event Info
Music – Genre: Trance Event Info	Music – SomaFM Event Info
Operator, Please Hold – DCG Social Event Info	Party Line (Call Center Village Party) Event Info
Policy Mixer Happy Hour Event Info	Queercon Mixer Event Info
SecKC the WHOLE WIDE WORLD Event Info	Slopcon Event Info
Social Engineering Community Village Party Event Info	The KEVOPS Sellout Pool Party II: Sponsored by Zyn Event Info
The Unofficial DEF CON Shoot Event Info	Toxic BBQ Event Info
VETCON 2026 PARTY Event Info	Welcome Party at The Industrial Event Info
Whose Slide Is It Anyway? Event Info	Women, gender non-conforming and non-binary meetup with The Diana Initiative Event Info

[Return to Index](#)

DEF CON Vendors Table

List by name of the Vendors that will be in the Vendor area at DEF CON 34

One Page [All Vendors](#) list with descriptions

defcon.org [Vendors](#) page

1BitSquared LLC Vendor Info	Cognitive Security Institute Vendor Info
Cryptocurrency Advocate Vendor Info	DEEPNET LLC Vendor Info
Electronic Cats Vendor Info	Electronic Frontier Foundation (EFF) Vendor Info
FREE-WILI, LLC (last year was Intrepid Control Systems) Vendor Info	Geist-Projekt/Crisiswear Vendor Info
Hacker Warehouse Vendor Info	Hak5 LLC Vendor Info
iFixit Inc Vendor Info	InDiPro Vendor Info
Keyport, Inc. Vendor Info	LowMesh LLC Vendor Info
Midwest Gadgets LLC Vendor Info	Miscreants Vendor Info
No Starch Press Inc Vendor Info	Octopwn Kft Vendor Info
Phreeli Company Vendor Info	PhysSec Education Education PhysSec Vendor Info
Rabbit-Labs LLC Vendor Info	Red Team Tools Vendor Info
REKCAH Publishing Vendor Info	Rogue's Roost LLC Vendor Info
Rokland LLC Vendor Info	Shadowvex Industries Vendor Info
Sneakreaper Industries LLC Vendor Info	Sparrows Manufacturing Co Vendor Info
The Calyx Institute Vendor Info	The Open Organisation of Lockpickers (TOOOL) Vendor Info
The Tor Project Vendor Info	Women in Security and Privacy (WISP) Vendor Info

[Return to Index](#)

DEF CON Exhibitors Table

List by name of the Exhibitors that will be in the Exhibitor area at DEF CON 34

One Page [All Exhibitors](#) list with descriptions

defcon.org [Exhibitors](#) page

You may need to scroll to the right to see all info

ANG Exhibitor Info	Capitol Technology University Exhibitor Info
DEF CON Training Exhibitor Info	Expel Exhibitor Info
Flare.io Exhibitor Info	Hack The Box Exhibitor Info
Horizon3 Exhibitor Info	Pentest-Tools.com Exhibitor Info
Promptfoo Exhibitor Info	SubImage Inc. Exhibitor Info
Tracebit Exhibitor Info	ZYN Exhibitor Info

[Return to Index](#)

DEF CON Communities Table

A group of people with common interests, but don't qualify as a Village, is a Community,

One Page [All Communities](#) list with descriptions

defcon.org [Communities](#) page

You may need to scroll to the right to see all info

.EDU Community Community Info	CodeBloom Community Info
DCNextGen Community Info	DEF CON Academy Community Info
DEF CON Groups (DCG) Community Info	Hackers With Disabilities (HDA) Community Info
Hackers.town Community Info	Hard Hat Brigade Community Info
IllumiCon Community Info	La Villa Community Info
Lonely Hackers Club Community Info	LOONG Community Community Info
Memorial Chamber Community Info	Middle Easterns & Africans in Cyber Security (MEACS) Community Info
Mobile Hacking Community Community Info	National Marrow Donor Program (Be the Match) Community Info
Nix Vegas Community Community Info	Noob Community Community Info
Operating Systems Community Community Info	OSINT For Good Community Community Info
OWASP Foundation Community Info	Queercon Community Lounge Community Info
Quiet Room with TDI & MHH Community Info	Retro Tech Community Community Info
Robotic Hacking Community Community Info	The Diana Initiative Community Info
VETCON Community Info	Women in Security and Privacy (WISP) Community Info

[Return to Index](#)

Links to DEF CON 34 related pages

Links

DEF CON . org Links

DEF CON [Main page](#)

DEF CON [FAQ](#)

DEF CON [Recent News](#)

DEF CON 34 [Training Signup](#)

DEF CON 34 [Villages](#)

DEF CON 34 [Communities](#)

DEF CON 34 [Contests](#)

DEF CON CTF [Benevolent Bureau of Birds - News Annoucement](#)

DEF CON [YouTube](#) channel, prev years talks

DEF CON [Forum Page](#) (limited official use)

Thanks to aNullValue and the NFO Node crew for providing access to their backend database. <claps> to their hard work!

Combined Schedules of DEF CON, Villages, and everything else DC34

Hacker Tracker - [Android](#) and [IOS](#) - the official DEF CON schedule app

[The ONE!](#) - A consolidated DEFCON 34 schedule in multiple file formats - html, PDF, CSV, ICAL, epub, mobi, Google calendar

info.defcon.org - the official DEF CON NFO Node site

Other Interesting Links

[DEF CON 34 Planning Highlights \(URLs of note\)](#)

DEF CON Hackers with Disabilities [Forum Topic](#) - [DC34 HDA for DC34 thread](#)

[@defconparties](#) - [calendar](#)

[defconmusic](#) - Schedule/News from the DC Artists & Entertainment (A&E) Department

[Official SoundTrack](#)

[DEFCONorg](#) Twitch stream

[defconmusic](#) [DEF CON Entertainment Twitch stream](#)

[defconmusic](#) [YouTube channel](#)

[DCTV](#) - DEF CON TV: Twitch streams and Hotel TV channels

[#badgelife](#) spreadsheet of unofficial badges for DC34 - [submit a new badge](#)

DEF CON [Shoot](#)

DEF CON [BBQ](#)

[@qumqats](#) Twitter [List of Village](#) accounts to assist in watching Village happenings

Other cons during [#SummerHackerCamp](#)

Blackhat	BS @BlackHatEvents	T @BlackHatEvents	FB Black Hat Events
BSides Las Vegas	BS @BSidesLV	T @BSidesLV	FB @BSidesLV
The Diana Initiative	BS @Dianainitiative	T @Dianainitiative	FB @dianainitiative

Guides/Tips/FAQs

[The Definitive Guide to DEF CON](#)

[DEF CON A&E - Resources - Rough Distances and Maps](#)

[DEF CON A&E - Resources - Packing List](#)

[Guide to Attending DEF CON 31](#)

[How to Survive Def Con 2022](#)

[OpSec For DEF CON 30](#)

[DCG 201 Hacker Double Summer 2023 Guides](#)

[Birds of a Feather-Resources for 2022 Hacker Summer Camp](#)

[Lonely Hackers Club - DEF CON n00b guide - reddit thread](#)

[The Lost Policymaker's Guide to Hacker Summer Camp](#)

[Holon DEF CON 30 Preparation](#)

[DEF CON: The Survival Guide](#)

[Preparing for "Hacker Summer Camp"](#)

[General / previous years](#)

[DEF CON for N00bs](#)

[JK-47 - BSidesLV & DEFCON Conference Tips](#)

[Just another DEF CON guide](#)

[HACKER SUMMER CAMP 2018 GUIDE](#)

[On Attending DefCon](#)
