



## 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 30.

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 vendor pitch events
- Nonspecific timed events. Unfortunately this means the contests aren't on the regular schedule.
- 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](mailto:qumqats@outel.org)

Have a good time at DEF CON 30!

# Index of DEF CON 30 Activities

---

## Maps and detailed Village Info

---

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 Village, start at the alphabetic top, or go to a specific Village.

### Village Talk List

AIV - ASV - BHV - BICV - BTV - CLV - CPV - DC - DDV - DL - HHV - HRV - IOTV - LPV - MIV - PLV - PT - PWV - RHV - SKY - SOC - WS

---

Descriptions and Info for all the talks.

### Talk Descriptions

---

The latest news from defcon.org

### DEF CON News

---

The answer to your questions about DEF CON overall and for this year.

### DEF CON FAQ

### DEF CON 30 FAQ

---

Links to DEF CON 30 related pages

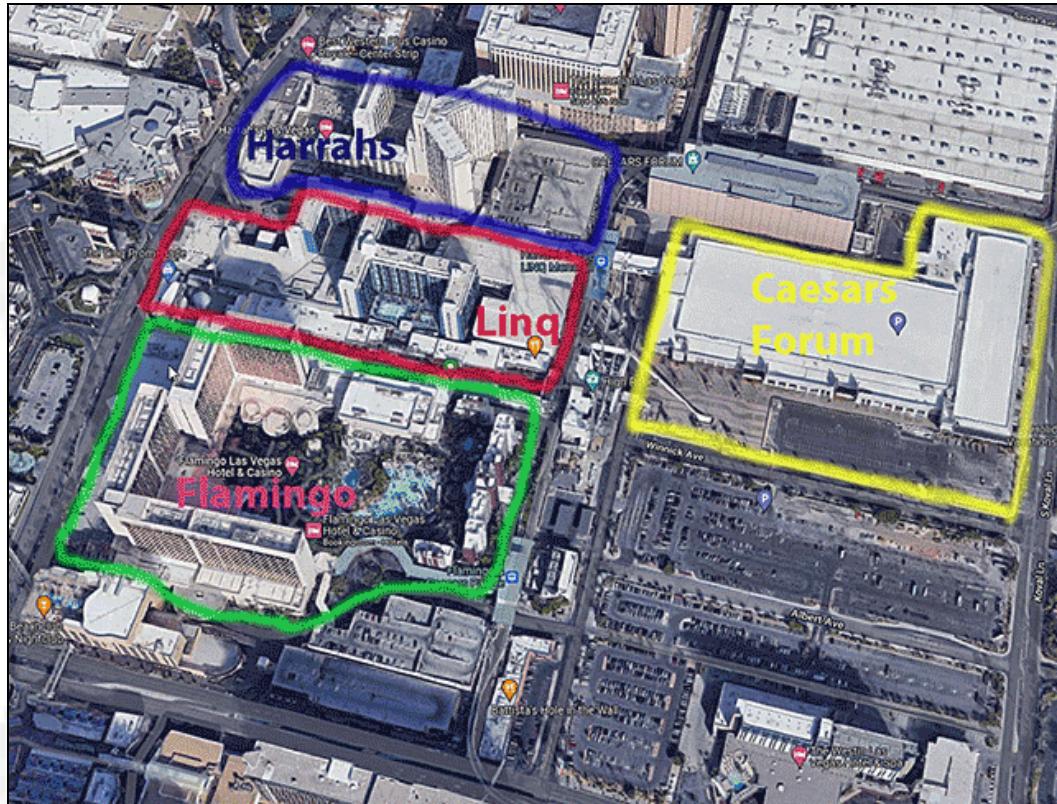
---

## Maps and detailed Village Info

---

Overview of the Hotels in the area of DEF CON 30

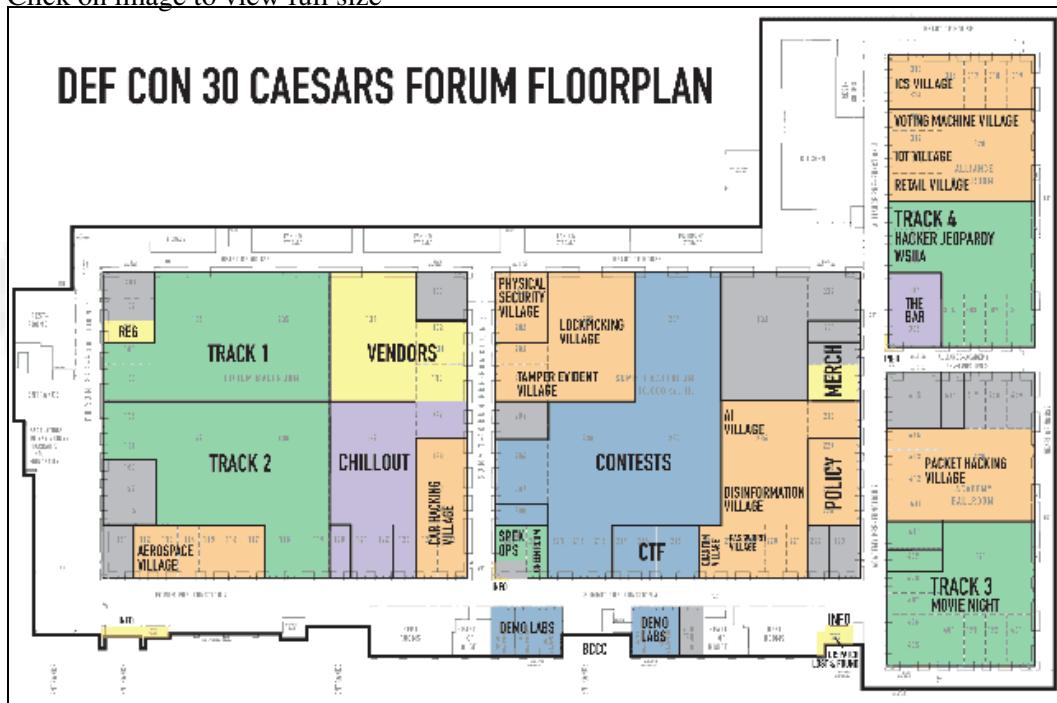
Click on image to view full size



Full floorplan of the Caesars Forum Convention Space

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

## DEF CON 30 CAESARS FORUM FLOORPLAN

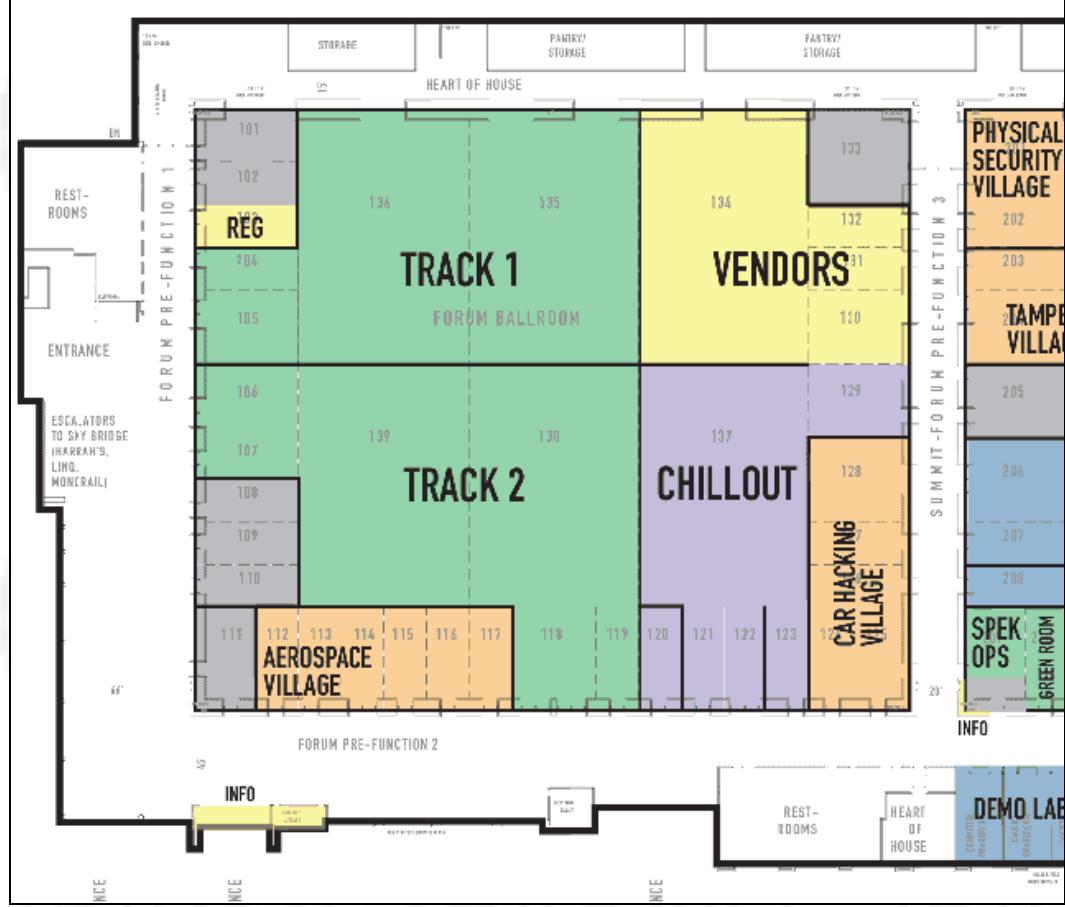


Closeup of the floorplan for the Caesars Forum, Forum Ballroom

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

# DEF CON 30 CAESARS FORUM FLOORPLAN

Forum BR, near/bottom of Sky Bridge Escalators

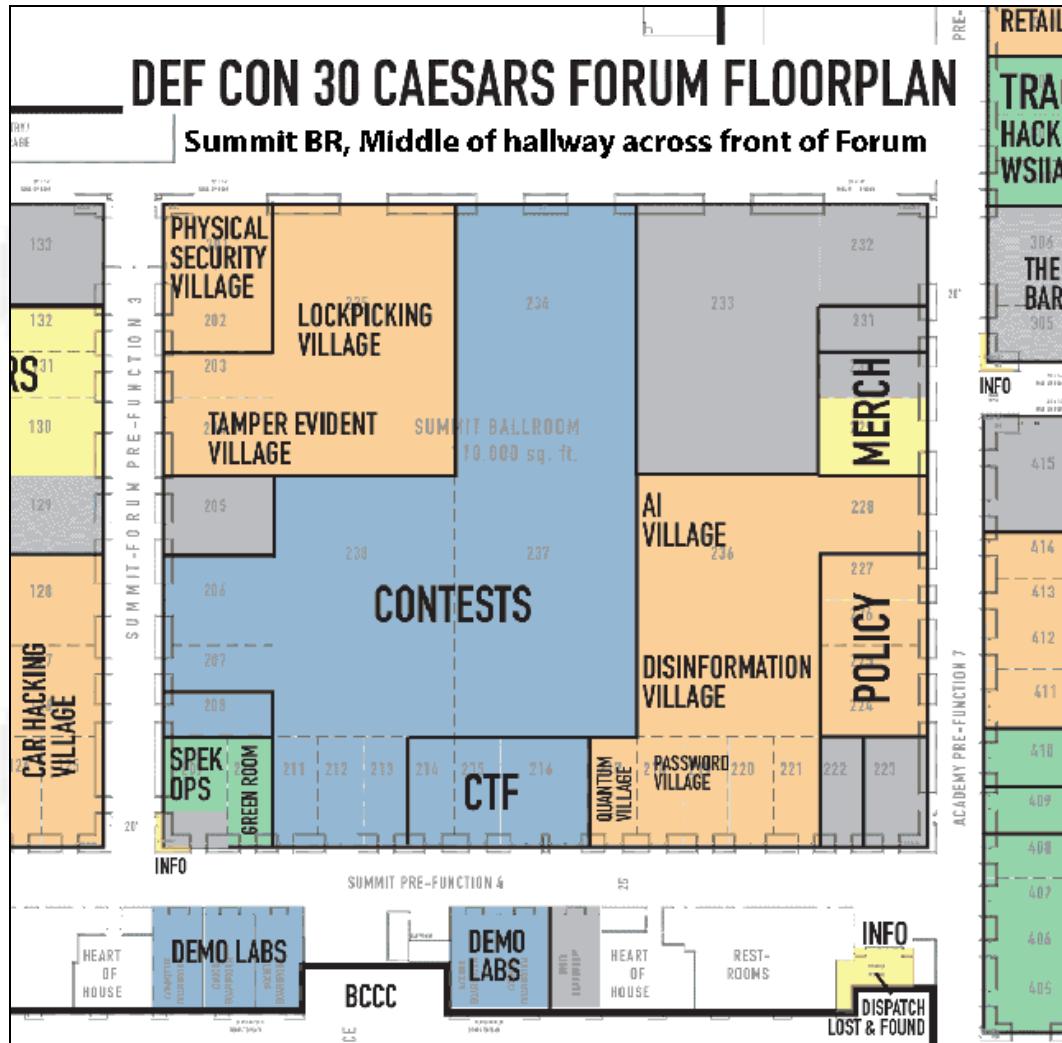


Closeup of the floorplan for the Caesars Forum, Summit Ballroom

Click on image to view full size

DEF CON 30 CAESARS FORUM FLOORPLAN

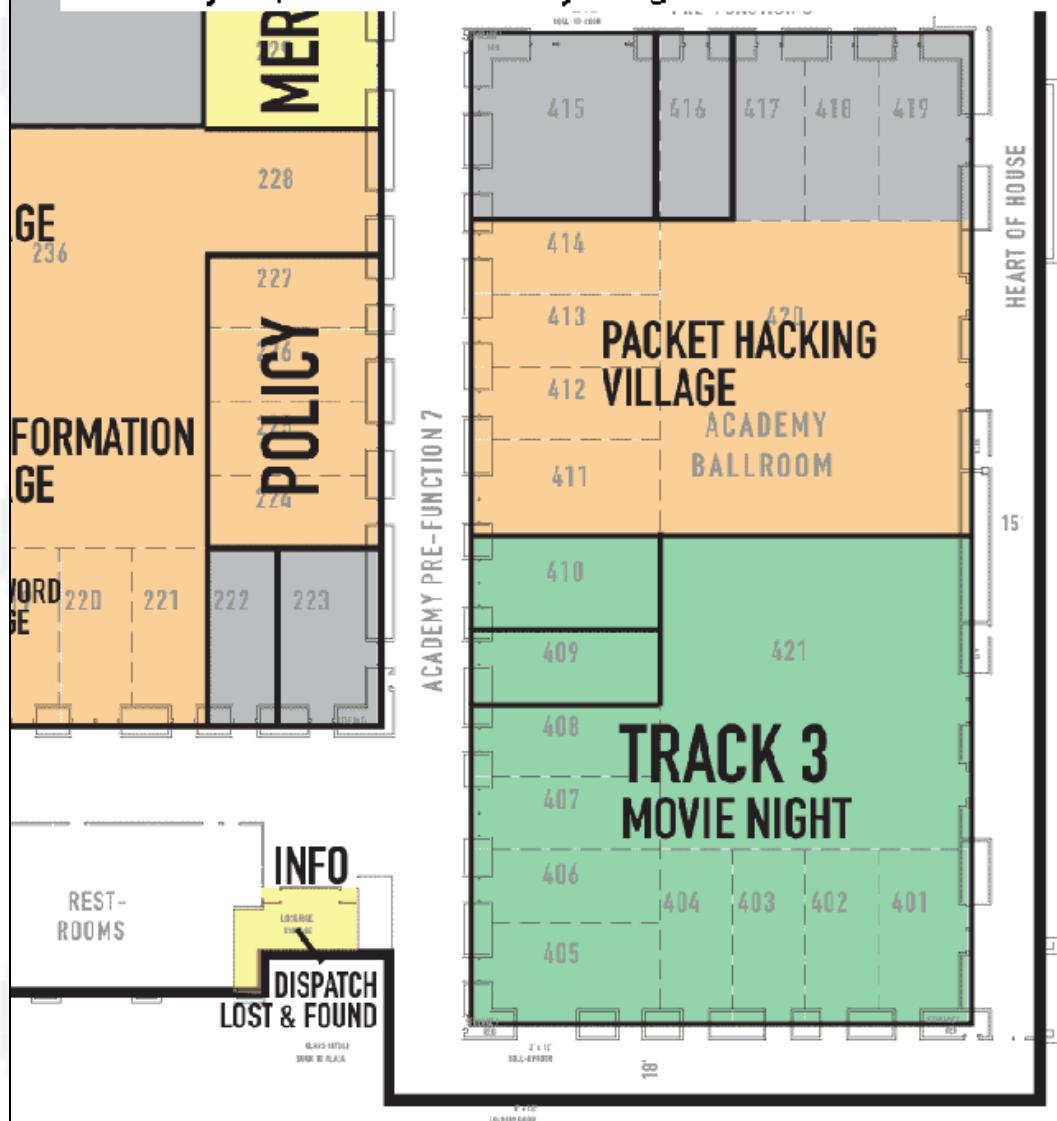
**Summit BR, Middle of hallway across front of Forum**



Closeup of the floorplan for the Caesars Forum, Academy Ballroom  
Click on image to view full size

# DEF CON 30 CAESARS FORUM FLOORPLAN

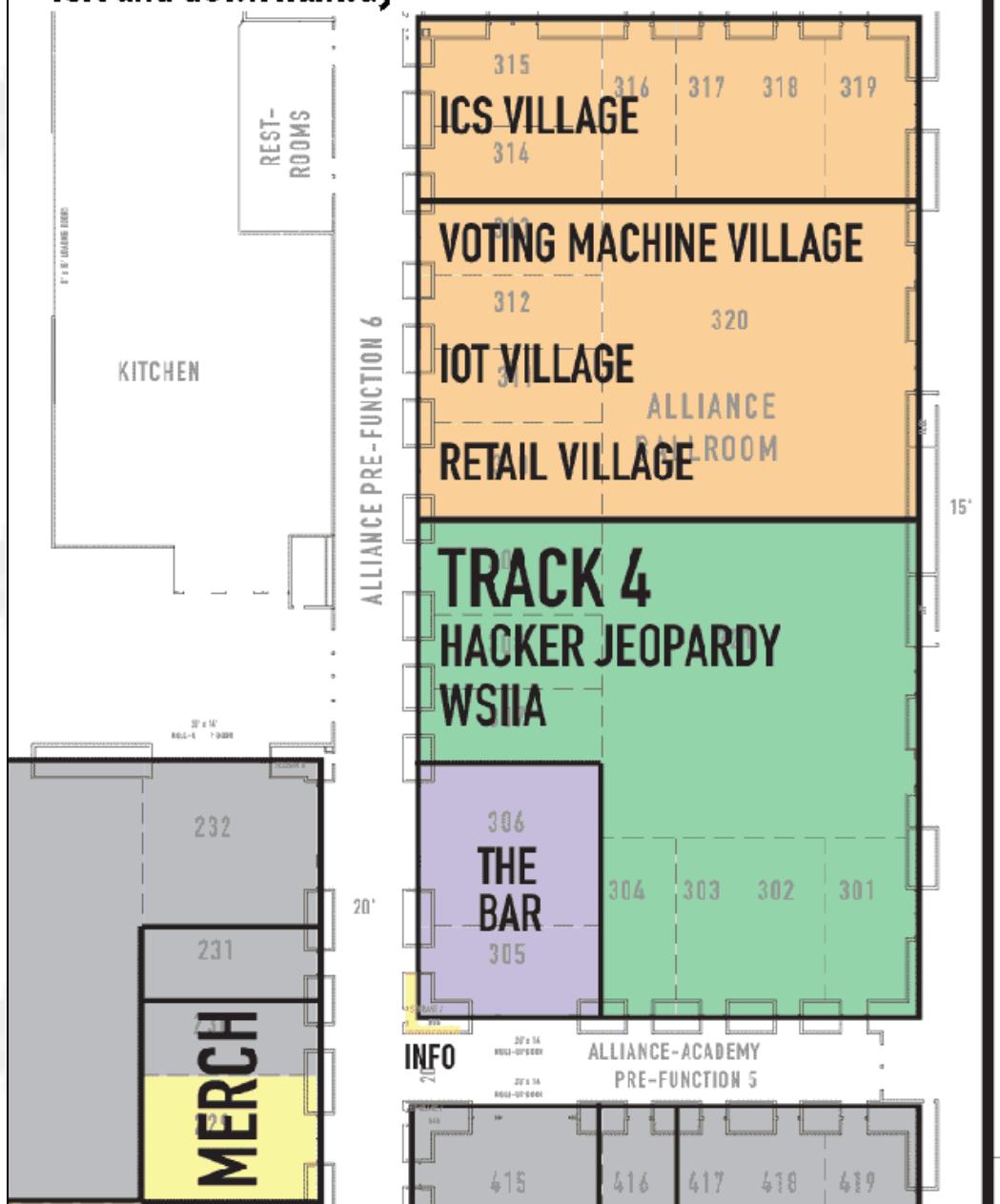
Academy BR, Far end from SkyBridge across front of Forum



Closeup of the floorplan for the Caesars Forum, Alliance Ballroom  
Click on image to view full size

# DEF CON 30 CAESARS FORUM FLOORPLAN

Alliance BR, Far end from SkyBridge across front of Forum,  
left and down hallway



Full floorplan for Flamingo  
Click on image to view full size

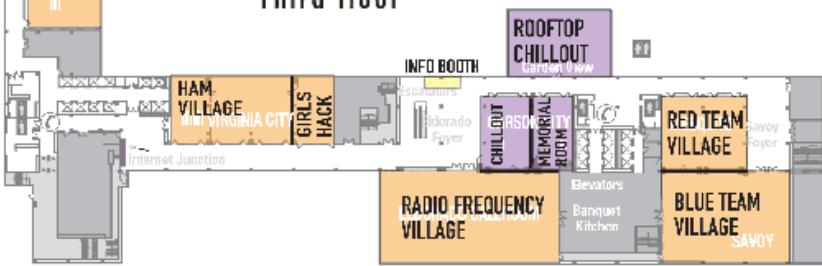
# DEF CON 30 FLAMINGO FLOORPLAN

EXECUTIVE CONFERENCE CENTER  
LOWER LEVEL



CORPORATE CONVENTION CENTER

Third floor



Closeup of the floorplan for the Caesars Forum, Alliance Ballroom  
Click on image to view full size

# DEF CON 30 FLAMINGO FLOORPLAN

CORPORATE CONVENTION CENTER

Third floor



Closeup of the floorplan for the Caesars Forum, Alliance Ballroom  
Click on image to view full size

# DEF CON 30 FLAMINGO FLOORPLAN

EXECUTIVE CONFERENCE CENTER

LOWER LEVEL



Full floorplan for Harrahs

Click on image to view full size

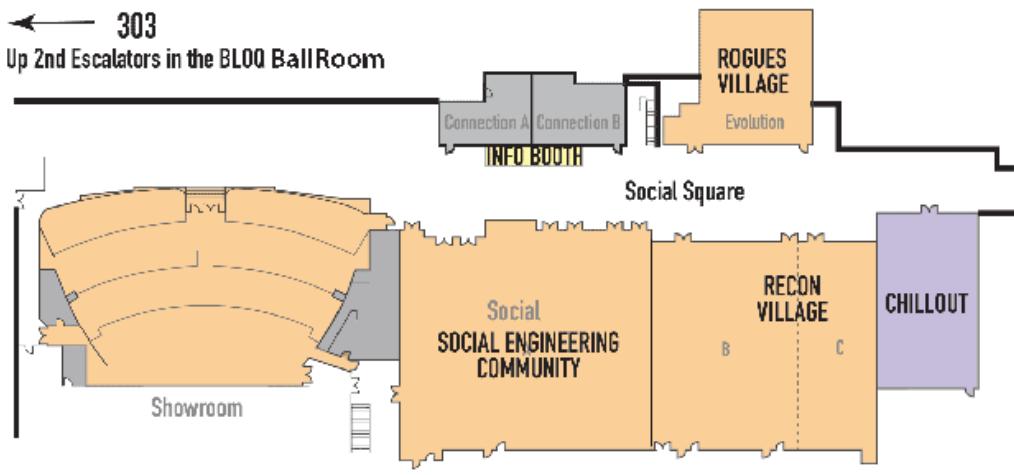
# DEF CON 30 HARRAH'S FLOORPLAN



Full floorplan for Linq  
Click on image to view full size

# DEF CON 30 LINQ FLOORPLAN

## Third Floor



## AIV - Artificial Intelligence Village

AIV Village Talk List:

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

Sched Page: <https://aivillage.org/defcon30/>

DC Forums Page: <https://forum.defcon.org/node/239784>

DC Discord Chan: <https://discord.com/channels/708208267699945503/732733090568339536>

Social Media Links:

TW [@aivillage\\_dc](#)

TI [@aivillage](#)

YT [link](#)

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

### A.I Village

DC29 Forum: <https://forum.defcon.org/node/236553>

Returning for DC 30!

<https://aivillage.org/>

[DEF CON Discord Channel](#)



Artificial Learning techniques are becoming more prevalent in core security technologies like malware detection and network traffic analysis. Its use has opened up new vectors for attacks against non-traditional targets, such as deep learning based image recognition systems used in self driving cars. There are unique challenges in defending and attacking these machine learning systems that the security community needs to be made aware of. This AI Village will introduce DEF CON attendees to these systems and the state of the art in defending and attacking them. We will provide a setting to educate DEF CON at large through workshops and a platform for researchers in this area to share the latest research.

Our main focus is on expanding the hands-on activities that attendees can participate in. This year, attendees will create a realistic face using StyleGAN, learn how to generate text, and attack a discriminatory resume screening program. We'll also have talks via CFP, and workshops: both introductory ML for beginners and intermediate/advanced on Facial Recognition/Adversarial ML. We are planning three contests inside the village: one as a standard CTF, another on evading a malware classifier (Ember), and a final realtime panel of Deepfaked DarkTangent's answering personal questions and giving opinions on life, the universe, and everything!

---

[Return to Index](#)

## APV - AppSec Village

APV Village [Talk List](#):

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

Sched Page: <https://www.appsecvillage.com/events/dc-2022>

DC Forums Page: <https://forum.defcon.org/node/240922>

DC Discord Chan: <https://discord.com/channels/708208267699945503/790973922949726228>

Social Media Links:

TW [@AppSec\\_Village](#)

LI [@appsecvillage](#)

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

The first three AppSec Villages were a resounding success. We learned that whether in person or online, our AppSec community is fantastic. We are pumped to be back bigger and better. Come immerse yourself in everything the world of application security has to offer. Whether you are a red, blue, or purple teamer, come learn from the best of the best to exploit software vulnerabilities and secure software. Software is everywhere, and Application Security vulnerabilities are lurking around every corner, making the software attack surface attractive for abuse. If you are just an AppSec n00b or launch deserialization attacks for fun and profit, you will find something to tickle your interest at the AppSec Village. Software runs the world. Everything from IoT, medical devices, the power grid, smart cars, voting apps - all of it has software behind it. Such a variety of topics will be reflected in our cadre of guest speakers representing all backgrounds and walks of life. AppSec

Village welcomes all travelers to choose from talks by expert community members, an all AppSec-focused CTF, contests that challenge your mind and your skillz, and more. Bring your thirst for knowledge and passion for breaking things, and your visit to AppSec Village will be a thrill!

---

[Return to Index](#)

---

## ASV - Aerospace Village

ASV Village [Talk List](#):

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

Sched Page: <https://aerospacevillage.org/events/upcoming-events/def-con-30/def-con-30-schedule/>

DC Forums Page: <https://forum.defcon.org/node/240500>

DC Discord Chan: <https://discord.com/channels/708208267699945503/732393044363444264>

Social Media Links:

TW [@secureaerospace](#)

LI [@aerospace-village](#)

TW [@hack\\_a\\_sat](#)

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



twitter: [@AppSec\\_Village](#)

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

CFP Link: <https://sessionize.com/appsec-village-dc30/>

The first three AppSec Villages were a resounding success. We learned that whether in person or online, our AppSec community is fantastic. We are pumped to be back bigger and better.

Come immerse yourself in everything the world of application security has to offer. Whether you are a red, blue, or purple teamer, come learn from the best of the best to exploit software vulnerabilities and secure software. Software is everywhere, and Application Security vulnerabilities are lurking around every corner, making the software attack surface attractive for abuse. If you are just an AppSec n00b or launch deserialization attacks for fun and profit, you will find something to tickle your interest at the AppSec Village.

Software runs the world. Everything from IoT, medical devices, the power grid, smart cars, voting apps - all of it has software behind it. Such a variety of topics will be reflected in our cadre of guest speakers representing all backgrounds and walks of

life.

AppSec Village welcomes all travelers to choose from talks by expert community members, an all AppSec-focused CTF, contests that challenge your mind and your skillz, and more. Bring your thirst for knowledge and passion for breaking things, and your visit to AppSec Village will be a thrill!

---

[Return to Index](#)

---

## AVV - Adversary Village

AVV Village [Talk List](#):

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

Sched Page: <https://adversaryvillage.org/adversary-events/DEFCON-30/>

DC Forums Page: <https://forum.defcon.org/node/239787>

DC Discord Chan: <https://discord.com/channels/708208267699945503/865456992101466192>

Social Media Links:

TW [@AdversaryVillag](#)

IG [@AdversaryVillage](#)LI [@adversaryvillage](#)FB [@AdversaryVillage](#)TI [@AdversaryVillage](#)DC <https://discord.gg/GDB3rC7KYz>YT [link](#)

### Adversary Village

DC29 Forum: <https://forum.defcon.org/node/236942>

Returning for DC 30!

Website: <https://adversaryvillage.org>

Twitter: <https://twitter.com/AdversaryVillag>

Adversary Village is a community initiative which purely focuses on Adversary simulation/emulation, threat/APT emulation, Breach and adversarial attack simulation, supply chain security simulation, adversary tactics, life, adversary philosophy, survival skills and Purple teaming. Adversary Village will be organizing technical talks, workshops, live demos, Adversary

Wars CTF, panel discussions and other hands-on activities on adversary simulation, emulation and purple teaming.

This is different from any of what has been covered in the existing villages, because our focus is on simulation of the actions of a threat actor or an adversary and this being simulated here. As this domain matures, we anticipate active participation from enterprises, as such simulations would help immensely towards internal capacity building from having a "live fire" training opportunity. An increasing number of researchers too are focusing on building tools and techniques for simulation of various adversarial actions against an organization or Supply chain, instead of actual real-world exploitation.

The goal of the Adversary Village would be to build a vendor neutral open security community for the researchers and organizations, who are putting together new means and methodologies towards the simulation/emulation of adversary tactics then purple teaming.

#### Adversary Wars CTF

Adversary Village will be hosting a CTF named "Adversary Wars", where the participants will have to pose as adversaries and simulate adversarial actions against each element of the dummy target organization.

Our end-goal is to build a CTF platform for adversary simulation/emulation knowledge sharing and exercises.

Adversary Wars would have real world simulation CTF scenarios and challenges, where the adversaries can simulate attacks and learn new attack vectors, TTPs, techniques, etc.

There would be combined exercises which include different levels of threat/adversary emulation and purple teaming.

#### Adversary Simulator booth

Adversary Simulator booth has hands-on adversary emulation plans specific to a wide variety of threat-actors, these are meant to provide the participant/visitor with a better understanding of the Adversary tactics.

This is a volunteer assisted activity where anyone, both management and technical folks can come-in and experience different categories of simulation, emulation and purple scenarios. Adversary Simulator booth will be having a lab environment focused on recreating enterprise infrastructure, aimed at simulation and emulating various adversaries. Visitors will be able to view, simulate and control various TTPs used by adversaries.

The simulator is meant to be a learning experience, irrespective of whether one is hands-on with highly sophisticated attack tactics or from the management.

---

[Return to Index](#)

## BHV - Bio Hacking Village

#### BHV VillageTalk List:

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

Sched Page: <https://www.villageb.io/2022bhvspeakers>

DC Forums Page: <https://forum.defcon.org/node/239958>

DC Discord Chan: <https://discord.com/channels/708208267699945503/735273390528528415>

Hours: Fri: 10:00 - 18:00 - Sat: 10:00 - 18:00 - Sun: 10:00 - 13:00

#### Social Media Links:

TW [@dc\\_bhv](#)

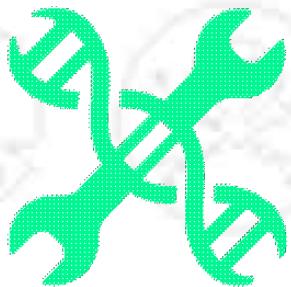
LI [@biohacking-village](#)

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

TI [@biohackingvillage](#)

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

SP [link](#)



# BIOHACKING VILLAGE

<https://villageb.io/>

**DEF CON Discord Channel**

CFP Link: <https://www.villageb.io/speaker-lab>

Growing from seeds of demand, the Biohacking Village emerged at DEF CON to deliver action-oriented reinvention of the safety and security of health care. **THE BIOHACKING VILLAGE**, a 501(c)3 organization, is uniquely poised to inform global conversations in health care cybersecurity research. Representing voices who see ‘code’ as genetics, ‘subroutines’ as organic processes, and ‘programs’ as life itself the BHV has grown to become an expansive and inclusive, hands-on playground for the entire biomedical ecosystem - patients, clinicians, hackers, manufacturers, regulators, hospital administrators, and others seeking healthier futures through meaningful technology. This nimble community delivers hands-on, strident learning labs to influence in health care, industry, and manufacturing.

**We bring the biomedical ecosystem to DEF CON in five ways:**

**DEVICE LAB :** The highly-collaborative environment builds health care, connecting security researchers, manufacturers, clinicians, and regulators, to learn from each other and develop skills, codifying best practices and paths for high fidelity cyber safety.

**SPEAKER LAB:** Speakers foster critical thinking, problem solving, human interaction literacy, ethics debates, creativity, and collaboration. Subject matter experts and researchers share the future of their research, reflecting the biological technologies and emerging threats.

**CATALYST LAB:** Providing interaction with thought leaders from the medical device and citizen science communities through training and hands-on workshops and solutions design, to cover the entirety of the biomedical device and security ecosystem.

**CAPTURE THE FLAG:** Featuring the virtual learning environment of St. Elvis Hospital, the CTF offers protocol, regulatory, and biological challenges to access and assess vulnerabilities in real devices.

**TABLE TOP EXERCISES:** Discussion-based sessions of increasing complexity and difficulty regarding vulnerabilities in a series of Machiavellian healthcare industry scenarios.

Attached Files



[Return to Index](#)

## BICV - Blacks in Cybersecurity

BICV VillageTalk List:

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

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

DC Forums Page: <https://forum.defcon.org/node/239775>

Social Media Links:

TW [@BlackInCyberCo1](#)

IG [@blackincyberconf](#)

TI [@blacksincybersecurity](#)

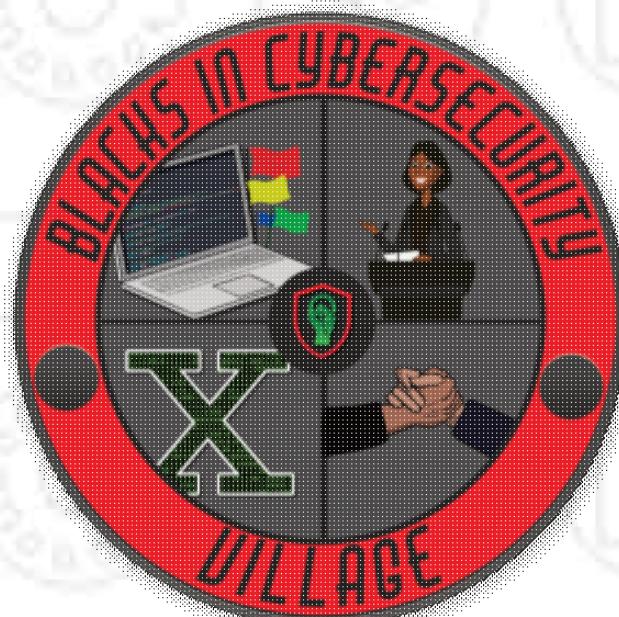
YT [link](#)

LI [@blackincyberconference](#)PT [@blacksincybersecurity](#)FB [@blackincyberconf](#)

Blacks In Cybersecurity (B.I.C) Village

PAST FORUM (not for this year:) DC29 Forum: <https://forum.defcon.org/node/236946>

Returning for DC 30!

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

The Blacks In Cybersecurity (BIC) 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 believe that we can normalize the discussion of deficiency and prejudices in Cybersecurity literacy, education and development that ultimately impact the progress and development of the field.

Our village programming is also designed to highlight Black experiences, innovations in the field, Black culture and Black history which is designed to encourage more diverse hobbyists and professionals to engage and contribute to this conference and the greater Cybersecurity and Hacker/Maker communities.

[Return to Index](#)

## BTV - Blue Team Village

BTV Village [Talk List](#):

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

Sched Page: <https://dc30.blueteamvillage.org/call-for-content-2022/schedule/#>

DC Forums Page: <https://forum.defcon.org/node/239776>

DC Discord Chan: <https://discord.com/channels/708208267699945503/732454317658734613>

Social Media Links:

TW [@BlueTeamVillage](#)

TI [@blueteamvillage](#)

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

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

**Blue Team Village**

DC29 Forum: <https://forum.defcon.org/node/236558>

Returning for DC30!



<https://blueteamvillage.org/>

[DEF CON Discord Channel](#)

We're still standing for our *fourth* DEF CON! Coming through the looking glass to showcase the defensive side of hacking, Blue Team Village is where you can find out all the multifarious facets of what it means to be a defender. You'll be able to teach and learn about the various ways to keep people safe - and how to subvert attacker expectations to turn their methods back on them.

You'll also be able to find community and mentor-ship within the defensive hacking paradigm, allowing you to find your path within this specialization to learning new skills and refining your old ones.

If you're looking for a community of like-minded hackers with a tendency towards forensics, threat hunting, and other blue-aligned topics, come celebrate the art of defensive hacking with us!

---

[Return to Index](#)

## CHV - Car Hacking Village

CHV VillageTalk List:

Home Page: <https://www.carhackingvillage.com/>  
Sched Page: <https://www.carhackingvillage.com/talks>  
DC Forums Page: <https://forum.defcon.org/node/240928>  
DC Discord Chan: <https://discord.com/channels/708208267699945503/732722838942777474>  
Social Media Links:  
TW [@CarHackVillage](#)  
DC <https://discord.gg/JWCcTAM>



Twitter: [@CarHackVillage](#)  
Website: <https://carhackingvillage.com/>

Learn, hack, play. The Car Hacking Village is an open, collaborative space to hack actual vehicles that you don't have to worry about breaking! Don't have tools? We'll loan you some. Never connected to a car? We'll show you how. Don't know where the controllers are? We'll show you how to take it apart. Want to learn more about automotive hacking and cyber security? Check out our talks. Want to hack mobility scooters? Yes! We'll do that to. Also, check out the CHV CTF.

Visit [carhackingvillage.com](https://carhackingvillage.com) for the latest information.

---

[Return to Index](#)

## CLV - Cloud Village

CLV VillageTalk List:

Home Page: <https://cloud-village.org/>  
Sched Page: <https://cloud-village.org/#talks>  
DC Forums Page: <https://forum.defcon.org/node/239788>  
DC Discord Chan: <https://discord.com/channels/708208267699945503/732733373172285520>

Social Media Links:

TW [@cloudvillage\\_dc](#)

YT [https://www.youtube.com/cloudvillage\\_dc](https://www.youtube.com/cloudvillage_dc)

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

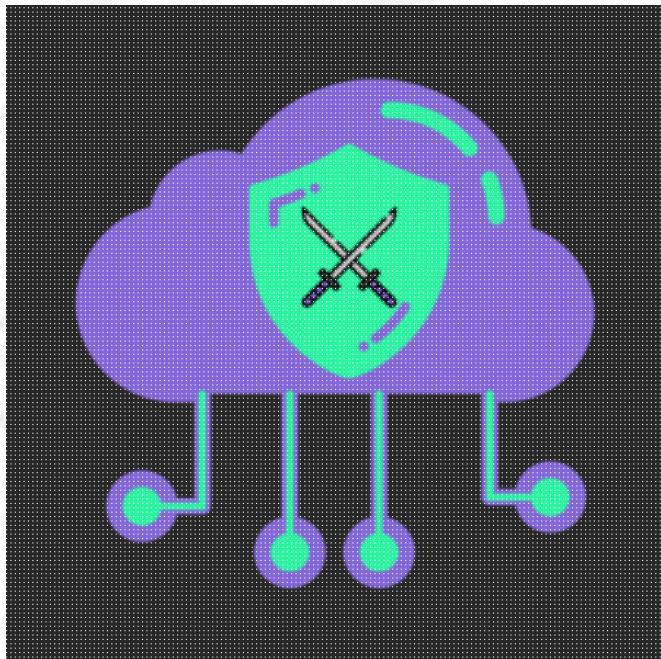
**Cloud Village**

DC29 Forum: <https://forum.defcon.org/node/236948>

Returning for DC30!

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

## DEF CON Discord Channel



With the industry shifting towards cloud infrastructure at a rapid speed, the presence of an open platform to discuss and showcase cloud research becomes a necessity.

Cloud village is an open platform for researchers interested in the area of cloud security. We plan to organize talks, tool demos, CTF and workshops around Cloud Security and advancements.

We will open Call for Papers/Workshops/Tools as soon as we get an approval from DEF CON.

Our CTF will be a jeopardy style 2.5 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.

---

[Return to Index](#)

## CON - Contests

---

CON Village[Talk List](#):

---

[Return to Index](#)

# CPV - Crypto Privacy Village

CPV Village Talk List:

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

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

DC Forums Page: <https://forum.defcon.org/node/239777>

DC Discord Chan: <https://discord.com/channels/708208267699945503/732734002011832320>

Social Media Links:

TW [@cryptovillage](#)

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

YT [link](#)

TI [@cryptovillage](#)

## Crypto & Privacy Village (CPV)

DC29 Forum: <https://forum.defcon.org/node/236562>

Returning for DC30!



<https://cryptovillage.org/>

<https://twitter.com/cryptovillage>

## DEF CON Discord Channel

At the Crypto & Privacy Village (CPV) you can learn how to secure your own systems while also picking up some tips and tricks on how to break classical and modern encryption. The CPV features workshops and talks on a wide range of cryptography and privacy topics from experts. We'll also have an intro to crypto talk for beginners, crypto-related games, the infamous CPV puzzle, a key-signing party, privacy-related art installations, and other great events like the Gold Bug Crypto Privacy Contest.

The CPV discusses the interesting intersection of privacy and technology as well as building privacy enhancing technologies. We are able to dig into the nitty gritty details of cryptography and give high level crypto intros for those who might feel intimidated by it. We also discuss and hack on major topics and issues: facial recognition technology, license plate readers, privacy enhancing clothing, crypto backdoor laws.

[Return to Index](#)

---

## DC - DEF CON Talks

DC VillageTalk List:

Home Page: <https://defcon.org/html/defcon-30/dc-30-index.html>

Sched Page: <https://defcon.org/html/defcon-30/dc-30-schedule.html>

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](#)

---

## DDV - Data Duplication Village

DDV VillageTalk List:

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

Sched Page: <https://dcddv.org/dc30-talk-schedule>

DC Forums Page: <https://forum.defcon.org/node/239778>

DC Discord Chan: <https://discord.com/channels/708208267699945503/732732641694056478>

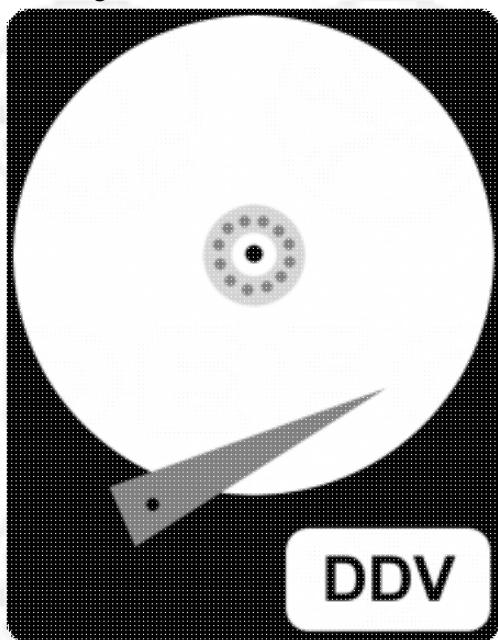
Social Media Links:

TW @DDV\_DC

**Data Duplication Village**

DC29 Forum: <https://forum.defcon.org/node/236520>

Returning for DC30!



Check the schedule and/or [dcddv.org](https://dcddv.org) for the most up-to-date information.

## DEF CON Discord Channel

It's true, the Data Duplication Village is back for DC 30! We have all the bits and bytes available from [infocon.org](http://infocon.org) packed up into nice, neat packages. If you're looking for something to fill up all your unused storage, may I recommend a nice hash table or two with a side of all of the DefCon talks? This is a "free-to-you" service where we're providing you direct access to terabytes of useful data to help build those skills.

### HOW IT WORKS

DEF CON will provide a core set of drive duplicators as well as data content options. We accept 6, 8, and 10TB drives on a first come, first served basis and duplicate 'till we can no longer see straight. Bring in your blank SATA3 drives - check them in early - to get the data you want. Come back in about 24 hours to pick up your data-packed drive. Space allowing, we'll accept drives all the way through until Saturday morning - but remember, it's FIFO!

- It will be a first come, first served to duplicate 'till we drop.
- Bring labeled 6TB SATA blank drives, and submit them in the queue for the data you want.
- Come back in 14-24 hours to pick up your data-packed drive.
- Space allowing, the last drop-offs will be no later than Saturday afternoon and the last drives will run overnight with the final pickup time at 11:30am.

### WHAT IS AVAILABLE - Three drives:

1. 6TB drive 1-3: Updated archive of [infocon.org](http://infocon.org) plus other "direct from DT" content, built on last years collection and always adding more for your data consuming appetite.
2. 6TB drive 2-3: freerainbowtables.com GSM A51 and MD5 hash tables (Tables 1-2) with about 404 gigs free
3. 6TB drive 3-3: more rainbowtables, lanman, mysqlsha1, ntlm, and some word lists (Tables 2-2) with about 136 gigs free

The DC 29 content will be posted at [dcddv.org](http://dcddv.org) once finalized

### WHAT YOU NEED

\* 6TB SATA3 512e format 7200rpm drive - one for each source you want

If you want a full copy of everything you will need three drives.

You can bring back last year's drive(s) to be wiped / updated (you should remove any 2018 stickers).

### WHEN TO BE THERE

Data Duplication Village Hours:

- Thursday, August 11, 16:00 - 19:00 (drop off only)
- Friday, August 12, 10:00 - 17:00
- Saturday, August 13, 10:00 - 17:00
- Sunday, August 14, 10:00 - 11:00 (last chance pickup only)

- Space permitting, last drop off is Saturday at 3:00pm.
- Last chance pickup is Sunday from 10:00 to 11:00.

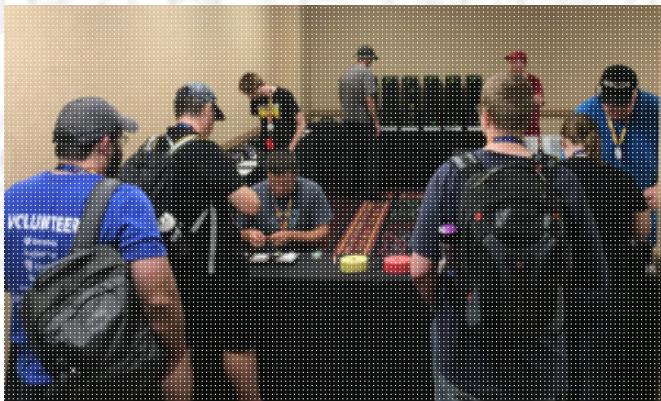
We're working on a method to post completed ticket ranges to <https://dcddv.org> and [https://twitter.com/DDV\\_DC](https://twitter.com/DDV_DC)

### SIDE NOTES

- Be aware that we cleared all the Vegas area stores of every single 6TB drive last year we did this so plan ahead and get them now!
- Duplicating a 6TB (About 5.46 usable) drive at an average of 120 Megabytes a second comes out to just under 14 hours per drive.
- With all about 16 duplicators going, we can duplicate about 95 drives concurrently.
- We're expect to push about 11GB per second out to the drives for 72 hours straight.
- We did 335 drives for DC24 and we're hoping to do even more at DC25!
- We are expecting more total duplicator capacity than last year!

## THAT'S ALL?

But wait - there's more! A few years ago, we made our stretch goal a reality to provide a pick-and-pull datastore in the DDV. We expect to do it bigger and better this year! [Dark Tangent](#) and [KnightOwl](#) post the up-to-date details in the DC Forum thread and you are encouraged to ask any questions you have there as con approaches.





---

[Return to Index](#)

---

## DL - DEF CON DemoLabs

DL Village [Talk List](#):  
Home Page: <https://forum.defcon.org/node/239774>

---

[Return to Index](#)

---

## GHV - Girls Hack Village

GHV Village [Talk List](#):  
Home Page: <https://www.blackgirlshack.org/girlshackvillage>  
DC Forums Page: <https://forum.defcon.org/node/240890>  
Social Media Links:  
TW @girlshackvllg  
IG @blackgirlshack



Girls Hack Village seeks to bring gender diverse perspectives of the contributions, perspectives, and issues facing women/girl hackers. It is a space to discuss issues affecting girls in cybersecurity and will include Talks, Workshops, and Discussions Panels. We are looking to have a village for womxn in ethical hacking fields that differ from organizations by focusing specifically on the experience of women as a diverse minority in cybersecurity.

Our village is designed to highlight the contributions and experiences of girls in cybersecurity. Women are underrepresented in cybersecurity and our goal is to highlight the female experience in Cybersecurity. Women are traditionally underrepresented at defcon and the girlshackvillage will give attendees the opportunity to learn about cybersecurity and hacking in a gender friendly place.

We will use the Discord to disseminate information during the village open hours and for Q&A during the discussion panel.

Twitter: <https://twitter.com/girlshackvllg>

Website: <https://www.blackgirlshack.org/girlshackvillage>

---

[Return to Index](#)

## HHV - Hardware Hacking and Soldering Skills Village

HHV Village Talk List:

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

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

DC Forums Page: <https://forum.defcon.org/node/239785>

DC Discord Chan: <https://discord.com/channels/708208267699945503/732728536149786665>

Social Media Links:

TW [@DC\\_HHV](#)

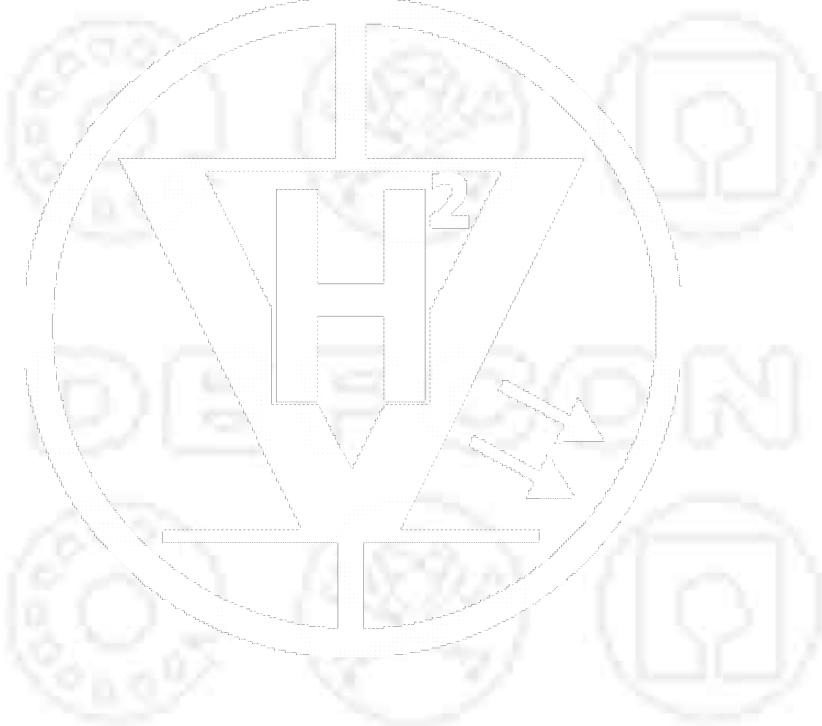
### Hardware Hacking and Soldering Skills Village

DC29 Forum: <https://forum.defcon.org/node/236591>

Returning for DC30!

<https://dchhv.org>

## DEF CON Discord



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.

We are two villages in one. We run a large number of tables for soldering when in person, and to allow people to understand that hardware is more than soldering we run the Hardware Hacking Village as embedded / reversing / hardware things other than soldering.

---

[Return to Index](#)

---

## HRV - Ham Radio Village

HRV Village [Talk List](#):

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

DC Forums Page: <https://forum.defcon.org/node/239779>

DC Discord Chan: <https://discord.com/channels/708208267699945503/732733631667372103>

Social Media Links:

TW [@HamRadioVillage](#)

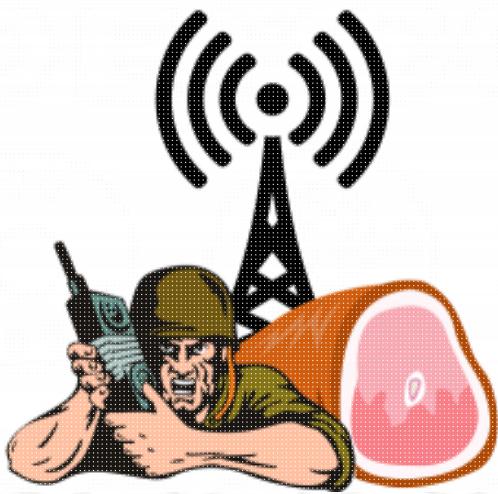
TI [@HamRadioVillage](#)

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

### Ham Radio Village & Exams

DC29 Forum: <https://forum.defcon.org/node/236589>

Returning for DC30!



<https://hamvillage.org/>

DEF CON Discord Channel

Ham radio isn't just what your grandpa does in the shed out back. Radios are an important piece of technology we use everyday, and amateur ("ham") radio has been at the forefront of its development since day one -- we are some of the original hardware hackers! DIY, exploration, and sharing has always been a vital part of our community and the goal of Ham Radio Village is to nurture this growth into the next generation with all of the amazing people at DEF CON.

Our village will have demos, talks, presentations, contests, and of course, license exams!

So come visit Ham Radio Village to learn more about the hobby, including how antennas work (and how to build your own), how to actually use that software defined radio sitting on the shelf, how to trackdown a rogue transmitter with a handheld radio, and how you can legally transmit 1,500 Watts into the airwaves after taking a simple multiple-choice test!

One of the unique things about ham radio is that it goes deep into the theory and science of radio. This knowledge unlocks a whole new level of understanding about why and how radios work and radio waves propagate. With just about everything containing some sort of radio these days, this information can help us better research, attack, and defend all things that emit RF. For example: Just about anyone can build an antenna with simple hardware; having an understanding of the fundamentals allows you to troubleshoot and tune the performance of that antenna to pick up the exact signals you want while filtering out the rest.

---

[Return to Index](#)

## ICSV - Industrial Control Systems Village

ICSV Village [Talk List](#):

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

Sched Page: <https://www.icsvillage.com/schedule-def-con-30>

DC Forums Page: <https://forum.defcon.org/node/239780>

DC Discord Chan: <https://discord.com/channels/708208267699945503/735938018514567178>

Social Media Links:

TW [@ICS\\_Village](#)

LI [@icsvillage](#)

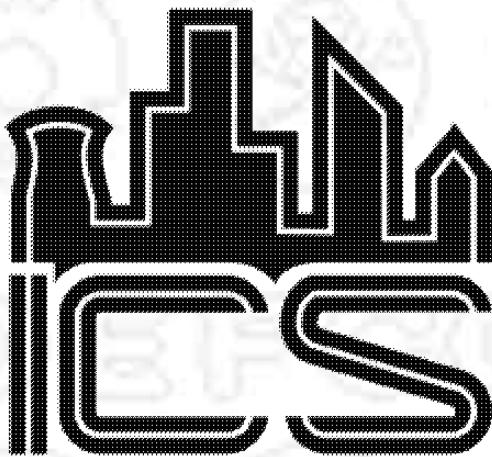
YT [link](#)

TI @ics\_village

ICS Village

DC29 Forum: <https://forum.defcon.org/node/236565>

Returning for DC30!



<https://www.csvillage.com/>

**DEF CON Discord Channel**

### **Mission.**

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

- Connecting public, industry, media, policymakers, and others directly with ICS systems and experts.
- Providing educational tools and materials to increase understanding among media, policymakers, and the general population.
- Providing access to ICS for security researchers to learn and test.
- Hands on instruction for industry to defend ICS systems.

### **Why.**

High profile Industrial Controls Systems security issues have grabbed headlines and sparked changes throughout the global supply chain. The ICS Village allows defenders of any experience level to understand these systems and how to better prepare and respond to the changing threat landscape.

### **Exhibits.**

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), 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!

---

[Return to Index](#)

# IOTV - Internet Of Things Village

IOTV Village Talk List:

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

Sched Page: <https://www.iotvillage.org/defcon.html>

DC Forums Page: <https://forum.defcon.org/node/239789>

DC Discord Chan: <https://discord.com/channels/708208267699945503/732734565604655114>

Social Media Links:

TW @iotvillage

TW @ISEsecurity

TW @Villageidiotlab

LI @iotvillage

TI @iotvillage

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

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

**IoT Village**

DC29 Forum: <https://forum.defcon.org/node/236567>

Returning for DC30!



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

Follow both ISE ( @ISEsecurity )

IoT Village ( @IoTvillage ) on Twitter for updates.

**DEF CON Discord Channel**

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 \(ISE\)](#), and the non-profit organization, [Village Idiot Labs \(VIL\)](#). [Watch IoT Village In Action](#) to get an idea of our content and our attendees.

Keep an eye out for The IoT RED ALERT Contest.

Check out the official [IoT Village Store](#) for all your IoT Village swag!

[Return to Index](#)

## LPV - Lock Pick Village

LPV VillageTalk List:

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

DC Forums Page: <https://forum.defcon.org/node/240931>

DC Discord Chan: <https://discord.com/channels/708208267699945503/732734164780056708>

Social Media Links:

TW @toool

TI @toool\_us

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



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

Discord: <https://discord.com/channels/7082082...34164780056708>

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, 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.

[Return to Index](#)

## MISC - Misc

MISC Village[Talk List](#):

[Return to Index](#)

## MIV - MisInformation Village

MIV Village[Talk List](#):

Home Page: <https://defcon.misinfocon.com/>

DC Forums Page: <https://forum.defcon.org/node/242022>

Social Media Links:

TW [@MisinfoVillage](#)

TW [@misinfocon](#)



[Details to be changed later: This is what I have so far:]

[]

The Misinformation Village aims to present a comprehensive overview of misinformation tactics, current campaigns, potential methods for defense and inoculation, and discussions of current and future campaigns. We seek to define, identify, understand, address, and combat misinformation, as well as strengthen online content credibility and information quality.

Site: <https://defcon.misinfocon.com/>

Twitter: [@misinfovillage](#)

[]

[Return to Index](#)

## MUS - Music

MUS VillageTalk List:

Home Page: <https://defconmusic.org>  
Sched Page: <https://defconmusic.org/sched.txt>

Social Media Links:

TW @defcon\_music

YT link

TI @defcon\_music

TI @defcon\_chill

Music Link All the Things: [https://www.twitch.tv/defcon\\_music](https://www.twitch.tv/defcon_music) [https://www.twitch.tv/defcon\\_chill](https://www.twitch.tv/defcon_chill)  
<http://www.defconmusic.org/>

---

[Return to Index](#)

## PHV - Packet Hacking Village

PHV VillageTalk List:

Home Page: <https://www.wallofsheep.com/>  
Sched Page: <https://www.wallofsheep.com/pages/dc30>  
DC Forums Page: <https://forum.defcon.org/node/239781>  
DC Discord Chan: <https://discord.com/channels/708208267699945503/708242376883306526>

Social Media Links:

TW @wallofsheep

FB @wallofsheep

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

TI @wallofsheep

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

**Packet Hacking Village**

DC29 Forum: <https://forum.defcon.org/node/236737>

Returning for DC30!



<https://www.wallofssheep.com/>

## DEF CON Discord Channel

### Packet Hacking Village

The Packet Hacking Village is an experience like no other. We are one of the longest-standing DEF CON villages, and we wear that honor with pride. The Packet Hacking Village is a place where everyone can take away some knowledge, whether they are a threat hunter, pentester, or an enthusiastic newcomer. We provide exciting events, live music, competitions with awesome prizes, and learning opportunities for all levels.

### Wall of Sheep

The Wall of Sheep is an entertaining and interactive demonstration of what happens when network users let their guard down.

People don't always think about internet safety in a practical sense. Even seasoned industry professionals get careless and believe that technology will passively protect them. The Wall of Sheep puts these assumptions to the test, and shows that when people let their guard down, anything can happen - and often does.

We monitor the DEF CON network, waiting for users to log into their email, web sites, or other network services without the protection of encryption. Once found, we post redacted yet identifiable information on the Wall of Sheep as a good-natured reminder that security matters, and someone is always watching.

### Capture The Packet

The time for those of hardened mettle is drawing near; are you prepared to battle?

Compete in the world's most challenging cyber defense competition based on the Aries Security cyber range. Tear through hundreds of bleeding-edge challenges, traverse a hostile enterprise-class network, and diligently analyze the findings to escape unscathed. Glory and prizes await those who emerge victorious from this upgraded labyrinth.

While Capture The Packet can easily scale for users of every level, for DEF CON we pull out all the stops and present our most fiendishly difficult puzzles. Capture The Packet has been a DEF CON Black Badge event for over 10 years, and we don't plan on stopping. This event attracts the best of the best from around the world to play – are you ready to show us what you've got?

### Packet Detective & Packet Inspector

DEF CON regularly attracts fresh talent in the Information Security field. Packet Detective and Packet Inspector engage experienced professionals and newcomers alike with hands-on, volunteer supported exercises.

These challenges promote critical thinking, teach core security tools, build professional cybersecurity skillsets, and inspire attendees towards larger Capture The Flag (or Packet!) style events.

Packet Detective and Packet Inspector are a great way for folks of all experience levels to learn under the eye of our skilled volunteers. Whether it's time to brush up on skills or time to launch a new career, this is the best place to start.

### Walkthrough Workshops

Walkthrough Workshops offer hands-on training at a self-guided pace. In these workshops, attendees take a deep dive into some of the most relevant subjects in cybersecurity with subject matter experts standing by to assist. Every year we bring new topics to the table, and our team of experts from all walks of life provide mentoring to guide the way.

### WosDJCo

At the Packet Hacking Village, we work hard to create a unique mood and vibe. The Wall of Sheep DJ Company (WoSDJCo) brings music and atmosphere into the mix. Our goal is to help everyone have a good time while staying entertained and motivated. Stop by and enjoy the smooth beats and deep vibes of musical hackery.

The **Packet Hacking Village** is where you'll find network shenanigans and a whole lot more. There's exciting events, live music, competitions with awesome prizes, and tons of giveaways. PHV welcomes all DEF CON attendees and there is something for every level of security enthusiast from beginners to those seeking a black badge. Wall of Sheep gives attendees a friendly reminder to practice safe computing through strong end-to-end encryption. PHV Speakers, Workshops, and Walkthrough Workshops delivers high quality content for all skill levels. Packet Detective and Packet Inspector offers hands-on exercises to help anyone develop or improve their Packet-Fu. WoSDJCo has some of the hottest DJs at con spinning live for your enjoyment. Finally... Capture The Packet, the ultimate cyber defense competition that has been honored by DEF CON as a black badge event for seven of the eight years of it's run.

---

[Return to Index](#)

## PLV - Policy Village

PLV Village [Talk List](#):

Sched Page: <https://forum.defcon.org/node/242912>

DC Village Page:

DC Forums Page: <https://forum.defcon.org/node/241813>

Policy@DEFCON

<https://www.defcon.org/html/links/dc-policy.html>

Hackers are early users and abusers of technology, and that technology is now critical to modern life. As governments make policy decisions about technology Hackers, researchers and academics need to be part of that conversation before decisions are made, not after policies are implemented. To do that DEF CON is a place for everyone on the policy and technology spectrum to interact, learn from each other, and improve technology.

Policy will build connections across and between technical and policy experts and provide opportunities for attendees interested in learning more about how policy and technology intersect and to examine the challenges at this intersection.

Our Policy program will consist of Main stage presentation and panels, daytime sessions in our policy track, and some evening lounges that will provide an off the record and more intimate setting to have policy-focused conversation

---

[Return to Index](#)

## PSV - Physical Security Village

PSV Village [Talk List](#):

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

DC Forums Page: <https://forum.defcon.org/node/240734>

DC Discord Chan: <https://discord.com/channels/708208267699945503/732732893830447175>

Social Media Links:

TW @bypassvillage

TI @bypassvillage



# LBV

<https://bypassvillage.org/>



Expect hours of operation at DEF CON:

- \* Friday: 11:00-18:00
- \* Saturday: 10:00-19:00
- \* Sunday: 10:00-13:00

The Physical Security Village (formerly the Lock Bypass 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.

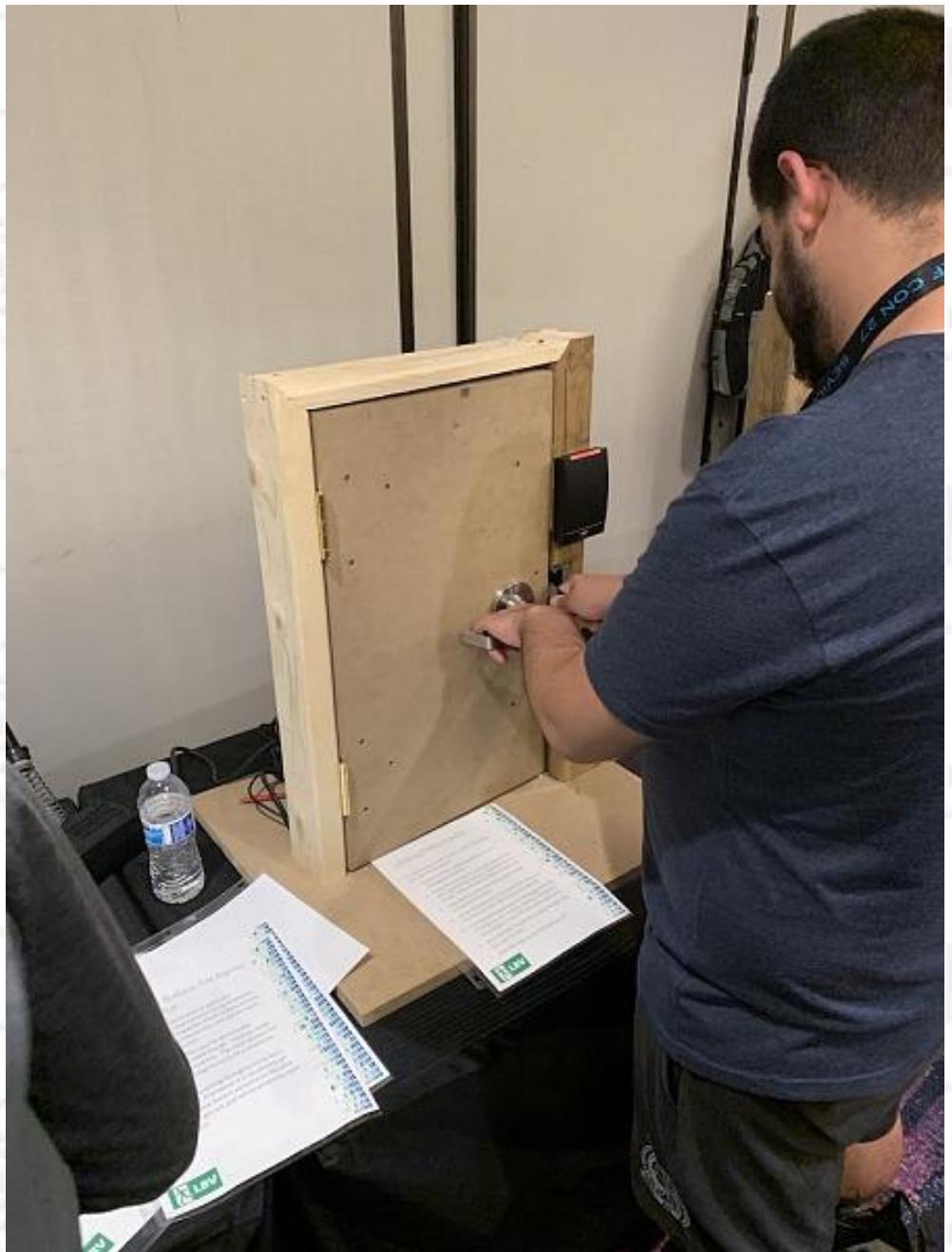
Looking for a challenge? Show us you can use lock bypass to escape from a pair of standard handcuffs in under 30 seconds and receive a prize!

How will you or your village contribute a new perspective to the content at DEF CON?

The Physical Security Village (formerly the Lock Bypass Village) is almost 100% hands on and is one of the only villages that has content about physical security. We strive to develop new content on a yearly basis to retain the interest of new and existing participants. This year we will be rebuilding all of our door displays to improve the production value, we will also have new displays that capture elevator security, double doors (with a deadbolt), forcible entry, some content on Access

controls/Wiegand/RFID cloning, and other subjects.









---

[Return to Index](#)

---

## PT - Paid Training

PT Village Talk List:

Home Page: <https://defcontrainings.myshopify.com/collections/all>

---

[Return to Index](#)

---

## PWV - Password Village

PWV Village Talk List:

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

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

DC Forums Page: <https://forum.defcon.org/node/240939>

DC Discord Chan: <https://discord.com/channels/708208267699945503/732733760742621214>

Social Media Links:

TW [@PasswordVillage](#)

TI [@passwordvillage](#)

YT [link](#)



Twitter: <https://twitter.com/passwordvillage>

Website: <https://passwordvillage.org/>

The Password Village provides training, discussion, and hands-on access to hardware and techniques utilized in modern password cracking, with an emphasis on how password cracking relates to your job function and the real world. No laptop? No problem! Feel free to use one of our terminals to access a pre-configured GPGPU environment to run password attacks against simulated real-world passwords. Village staff and expert volunteers will be standing by to assist you with on-the-spot training and introductions to Hashcat, as well as other FOSS cracking applications. Already a password cracking aficionado? Feel free to give a lightning talk, show off your skills, help a n00b learn the basics, or engage in riveting conversation with other password crackers.

---

[Return to Index](#)

---

## PYV - Payment Village

PYV VillageTalk List:

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

DC Forums Page: <https://forum.defcon.org/node/240942>

DC Discord Chan: <https://discord.com/channels/708208267699945503/732733473558626314>

Social Media Links:

TW @paymentvillage

TI @paymentvillage

YT link

[Image to be added later]

Twitter: <https://twitter.com/paymentvillage>

Website: <https://www.paymentvillage.org/>

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

Payment technologies are an integral part of our lives, yet few of us know much about them. Have you ever wanted to learn how payments work? Do you know how criminals bypass security mechanisms on Point of Sales terminals, ATM's and digital wallets?

Payment technologies are an integral part of our lives, yet few of us know much about them. Have you ever wanted to learn how payments work? Do you know how criminals bypass security mechanisms on Point of Sales terminals, ATM's and digital wallets? Come to the Payment Village and learn about the history of payments. We'll teach you how hackers gain access to banking endpoints, bypass fraud detection mechanisms, and ultimately, grab the money!

---

[Return to Index](#)

## QCV - Queercon

QCV VillageTalk List:

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

Social Media Links:

TW @Queercon

FB @126504813280

DC <https://discord.com/invite/jeG6Bh5>

---

[Return to Index](#)

## QTV - Quantum Village

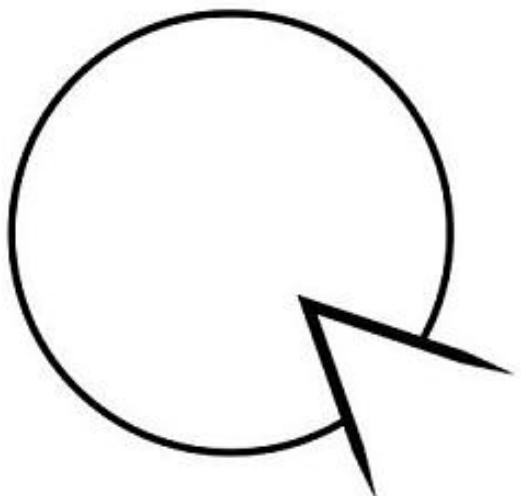
QTV VillageTalk List:

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

DC Forums Page: <https://forum.defcon.org/node/240893>

Social Media Links:

TW @quantum\_village



Village's twitter Handle: [@quantum\\_village](#)

Official web address/URL: <https://quantumvillage.io/>

CFP Link: Coming Soon.

Have you heard about 'Q-Day'? Or perhaps had someone tell you that 'Quantum is coming!' - well, they were right! Quantum Village is here! QV is a place to Engage, Explore, Discover, and Discuss 'Quantum Information Science & Technology' (QIST) from the hacker's point of view. Free from 'quantum woo' and sales pitches we have activities, talks, seminars, badges, stickers, and more for people to learn about this new and fast growing part of tech. From talks for experts to workshops for the newbie, if you want to get quantum aware we have something for you!

---

[Return to Index](#)

---

## RCV - Recon Village

RCV Village [Talk List](#):

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

Sched Page: <https://reconvillage.org/talks/>

DC Forums Page: <https://forum.defcon.org/node/239782>

DC Discord Chan: <https://discord.com/channels/708208267699945503/732733566051418193>

Social Media Links:

TW [@ReconVillage](#)

FB [@reconvillage](#)

### Recon Village

Returning for DC30!

DC29 Forum: <https://forum.defcon.org/node/236958>



**Website:** <https://reconvillage.org/>  
**Twitter:** <https://twitter.com/reconvillage> /  
**DEF CON Discord Channel**

Recon Village is an Open Space with Talks, Live Demos, Workshops, Discussions, CTFs, etc. with a common focus on Reconnaissance. The core objective of this village is to spread awareness about the importance of reconnaissance, open-source intelligence (OSINT), and demonstrating how even small information about a target can cause catastrophic damage to individuals and organizations.

We will have our Jeopardy Style OSINT CTF Contest again. The challenges will be around harvesting information about target organizations, their employee's social media profiles, their public svn/gits, password breach dumps, darknet, paste(s), etc. followed by active exploitation, bug hunting, investigation, and pentest scenarios of virtual targets. All the target organizations, employees, servers, etc. will be created by our team and hence will not attract any legal issues.

Similar to the last year, there will be Awesome rewards for CTF winners, along with free t-shirts, stickers, village coins, and other schwag which attendees can grab and show off.

---

[Return to Index](#)

## RFV - Radio Frequency Village

RFV Village [Talk List](#):  
Home Page: <https://rfhackers.com/>  
DC Forums Page: <https://forum.defcon.org/node/240934>  
DC Discord Chan: <https://discord.com/channels/708208267699945503/732732595493666826>  
Social Media Links:  
TW @rfhackers  
TW @rf\_ctf  
[link](#)  
DC <https://discordapp.com/invite/JjPQhKy>



Site: <https://rfhackers.com/>

Discord: <https://discord.com/channels/7082082...32595493666826>

(Formerly the Wireless Village)

Returning for DC30!

RF Hackers Sanctuary presents: The Radio Frequency Village at DEF CON .

After 14 years of evolution, from the WiFi Village, to the Wireless Village, RF Hackers Sanctuary presents: The Radio Frequency Village at DEF CON.

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, RFID, 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.

<https://rfhackers.com/the-crew>

Speaker and contest schedule can be found on our website:

<https://rfhackers.com/calendar>

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

---

[Return to Index](#)

## RHV - Retail Hacking Village

RHV Village [Talk List](#):

Home Page: <https://retailhacking.store/>

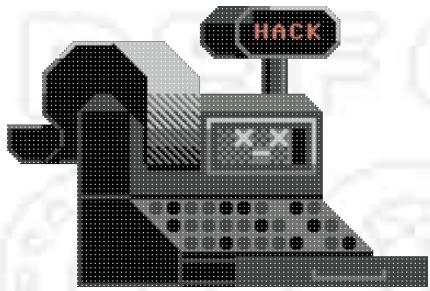
Sched Page: <https://retailhacking.store/schedule.html>

DC Forums Page: <https://forum.defcon.org/node/240887>

Social Media Links:

TW [@RetailHacking](#)

DC <https://discord.gg/DxG4Uj7WZV>



Have you ever wondered about the inner workings of point of sale systems, remote pricing handsets, and wireless wheel locking systems?

Then the Retail Hacking Village is for you!

Here you can test and hack various retail devices - all in the name of security research.

CFP: <https://retailhacking.store/events.html>

Twitter: <https://twitter.com/RetailHacking>

---

[Return to Index](#)

---

## **ROV - Rogues Village**

ROV Village [Talk List](#):

Home Page: <https://foursuits.co/roguesvillage>

Sched Page: <https://foursuits.co/roguesvillage>

DC Forums Page: <https://forum.defcon.org/node/239786>

DC Discord Chan: <https://discord.com/channels/708208267699945503/732732701144121434>

Social Media Links:

TW [@Rogues Village](#)

TI [@roguesvillage](#)

TW [@foursuits\\_co](#)

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

Returning for DC30!

DC29 Forum: <https://forum.defcon.org/node/236741>

<https://www.foursuits.co/roguesvillage>

<https://twitter.com/RoguesVillage>

[DEF CON Discord Channel](#)



Rogues Village is a place to explore alternative approaches and uses for security concepts, tools, and techniques by looking to non-traditional areas of knowledge. Incorporating expertise from the worlds of magic, sleight of hand, con games, and advantage play, this village has a special emphasis on the overlap between Social Engineering, Physical Security, and Playful Mischief.

Because we specialize in non-traditional approaches, Rogues Village can be an excellent entry point for people with a less established background in the security space. By introducing and engaging with existing topics in innovative, relatable, and frequently hands-on ways, they can become easier for people to approach and pick up for the first time.

Additionally, we are one of the few villages with a view that explicitly extends *beyond* the security space, meaning our perspective will necessarily include influences, ideas, and inspirations that are unique to Rogues Village.

---

[Return to Index](#)

---

## RTV - Red Team Village

RTV Village [Talk List](#):

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

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

DC Forums Page: <https://forum.defcon.org/node/240944>

Social Media Links:

TW [@RedTeamVillage\\_](#)

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

TI [@redteamvillage](#)

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

[Image to be added later]

Twitter: [https://twitter.com/RedTeamVillage\\_](https://twitter.com/RedTeamVillage_)

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

CFP: Coming Soon!

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. Hundreds of volunteers from around the world generate and share content with other offensively minded individuals in our workshops, trainings, talks, and conferences.

---

[Return to Index](#)

## SEV - Social Engineering Village

SEV Village [Talk List](#):

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

Sched Page: <https://www.se.community/village-schedule/>

DC Forums Page: <https://forum.defcon.org/node/240918>

DC Discord Chan: <https://discord.com/channels/708208267699945503/732733952867172382>

Social Media Links:

TW [@sec\\_defcon](#)

[Image/Logo/Iconography coming later]

The Social Engineering Community is formed by a group of individuals who have a passion to enable people of all ages and backgrounds interested in Social Engineering with a venue to learn, discuss, and practice this craft. We plan to use this opportunity at DEF CON to present a community space that offers those elements through panels, presentations, research opportunities, and contests in order to act as a catalyst to foster discussion, advance the craft and create a space for individuals to expand their network. SEC Village plans to accomplish the above by bringing together passionate individuals to have a shared stake in building this community.

For more information on our village stay tuned by following us at: [https://twitter.com/sec\\_defcon](https://twitter.com/sec_defcon)

Twitter: [https://twitter.com/sec\\_defcon](https://twitter.com/sec_defcon)

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

Call for Papers is open: <https://www.se.community/events/presentations/>

---

[Return to Index](#)

## SKY - SkyTalks - 303

SKY Village [Talk List](#):

Home Page: <https://skytalks.info/>

Sched Page: <https://skytalks2022.busyconf.com/schedule>

DC Forums Page: <https://forum.defcon.org/node/242039>

Social Media Links:

TW [@dcskytalks](#)

FB [@Skytalks](#)

303 Skytalks

Since DEF CON 16, Skytalks has been proud to bring you Old School DEF CON in a non-recorded, off-the-record track. Talks include technical deep dives, off-the-beaten path discussions, name-and-shame rants, cool technology projects, and plenty of shenanigans. We pride ourselves on a simple creed: “No recording. No photographs. No bullshit.”

Twitter: [@dcskytalks](#)

Website: <https://skytalks.info>

[]

---

[Return to Index](#)

## SOC - Social Activities: Parties/Meetups

SOC Village[Talk List](#):

---

[Return to Index](#)

## TEV - Tamper Evident Village

TEV Village[Talk List](#):

DC Forums Page: <https://forum.defcon.org/node/240937>

"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; an electronic tamper challenge. An extremely realistic explosive with traps, alarms, and a timer ticking down. One mistake and BOOM, you're dead. Make every second count! Sign ups on-site when the TEV begins.
- Tamper-Evident King of the Hill; a full-featured tamper challenge. Tamper single items at your leisure and attempt to beat the current best. There can be only ONE! No sign ups required, play on-site when the TEV begins.
- Badge Counterfeiting Contest; submit your best forgery of a DEF CON human badge. Other target badges are also available for those looking for more counterfeit fun!
- For your viewing pleasure, collections of high-security tamper-evident seals from around the world.
- Sit-down presentations & demonstrations on various aspects of tamper-evident seals and methods to defeat them.
- Hands-on fun with adhesive seals, mechanical seals, envelopes, and evidence bags.

(A change to this content may appear soon.)

---

[Return to Index](#)

## VMV - Voting Machine Village

VMV Village[Talk List](#):

DC Forums Page: <https://forum.defcon.org/node/239783>

DC Discord Chan: <https://discord.com/channels/708208267699945503/732733881148506164>

Social Media Links:

TW @votingvillagedc

YT link

## Voting Village

Returning for DC30!

DC29 Forum: <https://forum.defcon.org/node/236962>



<https://twitter.com/votingvillagedc>

<https://www.youtube.com/channel/UCnD...3sO8chqS5MGvwg>

## DEF CON Discord Channel

Voting Village explores voting machines, systems, and databases and works to promote a more secure democracy.

---

[Return to Index](#)

## WS - DEF CON Workshops

WS VillageTalk List:

Home Page: <https://forum.defcon.org/node/239773>

---

[Return to Index](#)

## Talk/Event Schedule

### Thursday

---

This Schedule is tentative and may be changed at any time. Check at an Info Booth for the latest.

## **Thursday - 00:00 PDT**

---

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

---

[IOTV](#) - IoT Village CTF Creator's Contest -

---

## **Thursday - 01:00 PDT**

---

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

---

[IOTV](#) - cont...(00:00-15:59 PDT) - IoT Village CTF Creator's Contest -

---

## **Thursday - 02:00 PDT**

---

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

---

[IOTV](#) - cont...(00:00-15:59 PDT) - IoT Village CTF Creator's Contest -

---

## **Thursday - 03:00 PDT**

---

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

---

[IOTV](#) - cont...(00:00-15:59 PDT) - IoT Village CTF Creator's Contest -

---

## **Thursday - 04:00 PDT**

---

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

---

[IOTV](#) - cont...(00:00-15:59 PDT) - IoT Village CTF Creator's Contest -

---

## **Thursday - 05:00 PDT**

---

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

---

[IOTV](#) - cont...(00:00-15:59 PDT) - IoT Village CTF Creator's Contest -

---

## **Thursday - 06:00 PDT**

---

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

---

[IOTV](#) - cont...(00:00-15:59 PDT) - IoT Village CTF Creator's Contest -

---

## **Thursday - 07:00 PDT**

---

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

---

DC - Human Registration Open

[IOTV](#) - cont...(00:00-15:59 PDT) - IoT Village CTF Creator's Contest -

---

## Thursday - 08:00 PDT

---

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

[DC](#) - cont...(07:00-19:59 PDT) - Human Registration Open

[IOTV](#) - cont...(00:00-15:59 PDT) - IoT Village CTF Creator's Contest -

## Thursday - 09:00 PDT

---

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

[DC](#) - cont...(07:00-19:59 PDT) - Human Registration Open

[IOTV](#) - cont...(00:00-15:59 PDT) - IoT Village CTF Creator's Contest -

[SOC](#) - Chillout Lounge - Entertainment - Rusty,s1gns0f1fe,Pie & Darren,Merin MC,Kampf,djdead

## Thursday - 10:00 PDT

---

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

[DC](#) - cont...(07:00-19:59 PDT) - Human Registration Open

[IOTV](#) - cont...(00:00-15:59 PDT) - IoT Village CTF Creator's Contest -

[SOC](#) - cont...(09:00-17:59 PDT) - Chillout Lounge - Entertainment - Rusty,s1gns0f1fe,Pie & Darren,Merin MC,Kampf,djdead

[WS](#) - The Purple Malware Development Approach - Olaf Hartong,Mauricio Velazco

[WS](#) - Network Hacking 101 - Victor Graf,Ben Kurtz

[WS](#) - Protect/hunt/respond with Fleet and osquery - Guillaume Ross,Kathy Satterlee

[WS](#) - Hands-On TCP/IP Deep Dive with Wireshark - How this stuff really works - Chris Greer

## Thursday - 11:00 PDT

---

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

[DC](#) - cont...(07:00-19:59 PDT) - Human Registration Open

[IOTV](#) - cont...(00:00-15:59 PDT) - IoT Village CTF Creator's Contest -

[SOC](#) - cont...(09:00-17:59 PDT) - Chillout Lounge - Entertainment - Rusty,s1gns0f1fe,Pie & Darren,Merin MC,Kampf,djdead

[WS](#) - cont...(10:00-13:59 PDT) - The Purple Malware Development Approach - Olaf Hartong,Mauricio Velazco

[WS](#) - cont...(10:00-13:59 PDT) - Network Hacking 101 - Victor Graf,Ben Kurtz

[WS](#) - cont...(10:00-13:59 PDT) - Protect/hunt/respond with Fleet and osquery - Guillaume Ross,Kathy Satterlee

[WS](#) - cont...(10:00-13:59 PDT) - Hands-On TCP/IP Deep Dive with Wireshark - How this stuff really works - Chris Greer

## Thursday - 12:00 PDT

---

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

[DC](#) - cont...(07:00-19:59 PDT) - Human Registration Open

[IOTV](#) - cont...(00:00-15:59 PDT) - IoT Village CTF Creator's Contest -

[SOC](#) - cont...(09:00-17:59 PDT) - Chillout Lounge - Entertainment - Rusty,s1gns0f1fe,Pie & Darren,Merin MC,Kampf,djdead

[SOC](#) - Friends of Bill W -

[WS](#) - cont...(10:00-13:59 PDT) - The Purple Malware Development Approach - Olaf Hartong,Mauricio Velazco

[WS](#) - cont...(10:00-13:59 PDT) - Network Hacking 101 - Victor Graf,Ben Kurtz

WS - cont...(10:00-13:59 PDT) - [Protect/hunt/respond with Fleet and osquery](#) - Guillaume Ross,Kathy Satterlee  
WS - cont...(10:00-13:59 PDT) - [Hands-On TCP/IP Deep Dive with Wireshark - How this stuff really works](#) - Chris Greer

## Thursday - 13:00 PDT

---

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

---

DC - cont...(07:00-19:59 PDT) - Human Registration Open  
IOTV - cont...(00:00-15:59 PDT) - [IoT Village CTF Creator's Contest](#) -  
SOC - cont...(09:00-17:59 PDT) - [Chillout Lounge - Entertainment](#) - Rusty,s1gns0f1fe,Pie & Darren,Merin  
MC,Kampf,djdead  
WS - cont...(10:00-13:59 PDT) - [The Purple Malware Development Approach](#) - Olaf Hartong,Mauricio Velazco  
WS - cont...(10:00-13:59 PDT) - [Network Hacking 101](#) - Victor Graf,Ben Kurtz  
WS - cont...(10:00-13:59 PDT) - [Protect/hunt/respond with Fleet and osquery](#) - Guillaume Ross,Kathy Satterlee  
WS - cont...(10:00-13:59 PDT) - [Hands-On TCP/IP Deep Dive with Wireshark - How this stuff really works](#) - Chris Greer

## Thursday - 14:00 PDT

---

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

---

DC - cont...(07:00-19:59 PDT) - Human Registration Open  
IOTV - cont...(00:00-15:59 PDT) - [IoT Village CTF Creator's Contest](#) -  
SOC - cont...(09:00-17:59 PDT) - [Chillout Lounge - Entertainment](#) - Rusty,s1gns0f1fe,Pie & Darren,Merin  
MC,Kampf,djdead

## Thursday - 15:00 PDT

---

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

---

DC - cont...(07:00-19:59 PDT) - Human Registration Open  
IOTV - cont...(00:00-15:59 PDT) - [IoT Village CTF Creator's Contest](#) -  
SOC - cont...(09:00-17:59 PDT) - [Chillout Lounge - Entertainment](#) - Rusty,s1gns0f1fe,Pie & Darren,Merin  
MC,Kampf,djdead  
WS - [Introduction to Software Defined Radios and RF Hacking](#) - Rich  
WS - [Pentesting Industrial Control Systems 101: Capture the Flag!](#) - Arnaud Soullie,Alexandrine Torrents  
WS - [House of Heap Exploitation](#) - Nathan Kirkland,Maxwell Dulin,Kenzie Dolan,Zachary Minneker  
WS - [Introduction to Azure Security](#) - Nishant Sharma,Jeswin Mathai

## Thursday - 16:00 PDT

---

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

---

DC - cont...(07:00-19:59 PDT) - Human Registration Open  
DDV - [DDV starts accepting drives for duplication](#) -  
SOC - cont...(09:00-17:59 PDT) - [Chillout Lounge - Entertainment](#) - Rusty,s1gns0f1fe,Pie & Darren,Merin  
MC,Kampf,djdead  
SOC - [Queercon Mixer](#) -  
SOC - [Toxic BBQ](#) -  
WS - cont...(15:00-18:59 PDT) - [Introduction to Software Defined Radios and RF Hacking](#) - Rich  
WS - cont...(15:00-18:59 PDT) - [Pentesting Industrial Control Systems 101: Capture the Flag!](#) - Arnaud Soullie,Alexandrine Torrents  
WS - cont...(15:00-18:59 PDT) - [House of Heap Exploitation](#) - Nathan Kirkland,Maxwell Dulin,Kenzie Dolan,Zachary Minneker

## Thursday - 17:00 PDT

---

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

[DC](#) - cont...(07:00-19:59 PDT) - Human Registration Open

[DDV](#) - cont...(16:00-18:59 PDT) - [DDV starts accepting drives for duplication](#) -

[SOC](#) - cont...(09:00-17:59 PDT) - [Chillout Lounge - Entertainment](#) - Rusty,s1gns0f1fe,Pie & Darren,Merin

MC,Kampf,djdead

[SOC](#) - cont...(16:00-17:59 PDT) - [Queercon Mixer](#) -

[SOC](#) - [Friends of Bill W](#) -

[SOC](#) - cont...(16:00-21:59 PDT) - [Toxic BBQ](#) -

[WS](#) - cont...(15:00-18:59 PDT) - [Introduction to Software Defined Radios and RF Hacking](#) - Rich

[WS](#) - cont...(15:00-18:59 PDT) - [Pentesting Industrial Control Systems 101: Capture the Flag!](#) - Arnaud Soullie,Alexandrine Torrents

[WS](#) - cont...(15:00-18:59 PDT) - [House of Heap Exploitation](#) - Nathan Kirkland,Maxwell Dulin,Kenzie Dolan,Zachary Minneker

[WS](#) - cont...(15:00-18:59 PDT) - [Introduction to Azure Security](#) - Nishant Sharma,Jeswin Mathai

## Thursday - 18:00 PDT

---

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

[DC](#) - cont...(07:00-19:59 PDT) - Human Registration Open

[DDV](#) - cont...(16:00-18:59 PDT) - [DDV starts accepting drives for duplication](#) -

[SOC](#) - [Thursday Opening Party - Entertainment](#) - FuzzyNop,Archwisp,DJ St3rling,Dr. McGrew,Magician Kody Hildebrand,NPC Collective,TRIODE,Ytcracker

[SOC](#) - [DC702 Pwnagotchi Party](#) -

[SOC](#) - cont...(16:00-21:59 PDT) - [Toxic BBQ](#) -

[WS](#) - cont...(15:00-18:59 PDT) - [Introduction to Software Defined Radios and RF Hacking](#) - Rich

[WS](#) - cont...(15:00-18:59 PDT) - [Pentesting Industrial Control Systems 101: Capture the Flag!](#) - Arnaud Soullie,Alexandrine Torrents

[WS](#) - cont...(15:00-18:59 PDT) - [House of Heap Exploitation](#) - Nathan Kirkland,Maxwell Dulin,Kenzie Dolan,Zachary Minneker

[WS](#) - cont...(15:00-18:59 PDT) - [Introduction to Azure Security](#) - Nishant Sharma,Jeswin Mathai

## Thursday - 19:00 PDT

---

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

[DC](#) - cont...(07:00-19:59 PDT) - Human Registration Open

[SOC](#) - cont...(18:00-20:59 PDT) - [DC702 Pwnagotchi Party](#) -

[SOC](#) - cont...(16:00-21:59 PDT) - [Toxic BBQ](#) -

## Thursday - 20:00 PDT

---

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

[SOC](#) - cont...(18:00-20:59 PDT) - [DC702 Pwnagotchi Party](#) -

[SOC](#) - cont...(16:00-21:59 PDT) - [Toxic BBQ](#) -

## Thursday - 21:00 PDT

---

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

---

SOC - [Hallway Monitor Party - Entertainment](#) - Tavoo,PankleDank,Heckseven,DotOrNot,CodexMafia

SOC - cont...(16:00-21:59 PDT) - [Toxic BBQ](#) -

## Friday

---

This Schedule is tentative and may be changed at any time. Check at an Info Booth for the latest.

---

### Friday - 06:00 PDT

---

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

---

SOC - [DEF CON Bike Ride "CycleOverride"](#) -

### Friday - 08:00 PDT

---

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

---

DC - Human Registration Open

### Friday - 09:00 PDT

---

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

---

AIV - [Opening Remarks on the State of AI & Security](#) - Brian Pendleton,Sven Cattell

AIV - (09:30-10:50 PDT) - [Automate Detection with Machine Learning](#) - Gavin Klondike

ASV - [California CyberSecurity Institute Space Grand Challenge](#) -

DC - cont...(08:00-18:59 PDT) - Human Registration Open

DC - [Merch \(formerly swag\) Area Open -- README](#) -

SKY - (09:30-10:20 PDT) - [Combatting sexual abuse with threat intelligence techniques](#) - Aaron DeVera

SOC - [Chillout Lounge - Entertainment](#) - Rusty,s1gns0f1fe,Pie & Darren,Merin MC,Kampf,djdead

### Friday - 10:00 PDT

---

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

---

AIV - cont...(09:30-10:50 PDT) - [Automate Detection with Machine Learning](#) - Gavin Klondike

ASV - cont...(09:00-16:59 PDT) - [California CyberSecurity Institute Space Grand Challenge](#) -

ASV - [Hack the Airport with Intelligenesis](#) -

ASV - [Hack the Airfield with DDS](#) -

ASV - [Satellite Eavesdropping with DDS](#) -

ASV - [Red Balloon Failsat Challenges](#) -

ASV - [Pen Test Partners A320 Simulator](#) -

ASV - [Hack-A-Sat Digital Twin Workshop](#) -

ASV - [Hack-A-Sat Team](#) -

ASV - [Amazon Web Services Aerospace and Satellite Jam](#) -

ASV - Boeing ARINC 429 Airplane Challenge and CTF -

BHV - BioHacking Village Keynote - Nina Alli

BHV - (10:30-10:59 PDT) - A Capitalist approach to hospital security - Eirick Luraas

BICV - The GACWR Story: Building a Black Owned Cyber Range - Jovonni Pharr,GACWR Team

BTW - Blue Team Village Opening Ceremony -

BTW - (10:30-11:30 PDT) - Obsidian Live: Eating the Elephant 1 byte at a Time - aviditas,ChocolateCoat

BTW - (10:30-11:30 PDT) - Obsidian Forensics: Kill Chain 1 Endpoint Forensics Walkthrough - Omenscan

BTW - (10:30-11:30 PDT) - Obsidian CTH: Go Phish: Visualizing Basic Malice - SamunoskeX

CLV - Cloud Village Opening Note - Jayesh Singh Chauhan

CLV - Automating Insecurity in Azure - Karl Fosaaen

CLV - (10:50-11:30 PDT) - Making the most of Microsoft cloud bug bounty programs: How I made in \$65,000 USD in bounties in 2021 - Nestori Syynimaa

CPV - (10:30-10:59 PDT) - Back to School! Hello RSA... and beyond! - Mike Guirao

DC - Old Malware, New tools: Ghidra and Commodore 64, why understanding old malicious software still matters - Cesare Pizzi

DC - Computer Hacks in the Russia-Ukraine War - Kenneth Geers

DC - (10:30-11:15 PDT) - OopsSec -The bad, the worst and the ugly of APT's operations security - Tomer Bar

DC - cont...(08:00-18:59 PDT) - Human Registration Open

DC - Panel - "So It's your first DEF CON" - How to get the most out of DEF CON, What NOT to do. - DEF CON Goons

DC - Panel - DEF CON Policy Dept - What is it, and what are we trying to do for hackers in the policy world? - DEF CON Policy Dept

DC - Vendor Area Open

DC - cont...(09:00-15:59 PDT) - Merch (formerly swag) Area Open -- README -

DC - Village Areas Open (Generally) -

DDV - DDV open and accepting drives for duplication -

DL - TheAllCommander - Matthew Handy

DL - Access Undenied on AWS - Noam Dahan

DL - Vajra - Your Weapon To Cloud - Raunak Parmar

DL - FISSURE: The RF Framework - Christopher Poore

DL - Zuthaka: A Command & Controls (C2s) integration framework - Lucas Bonastre,Alberto Herrera

HHV - Solder Skills Village - Open

HHV - Uwb Security Primer: Rise Of A Dusty Protocol - Göktay Kaykusuz

HHV - Hardware Hacking Village - Open

IOTV - Hands on Hardware Hacking – eMMC to Root - Deral Heiland

IOTV - Drone Hack -

IOTV - IoT Village CTF -

IOTV - IoT Village CTF Challenges -

IOTV - Hands on hacking labs -

LPV - (10:15-10:45 PDT) - Intro to Lockpicking - TOOOL

MIV - The hybrid strategies of autocratic states: narrative characteristics of disinformation campaigns in relation to issues of a scientific-health nature - Carlos Galán

SKY - cont...(09:30-10:20 PDT) - Combatting sexual abuse with threat intelligence techniques - Aaron DeVera

SKY - (10:35-11:25 PDT) - Hundreds of incidents, what can we share? - Brenton Morris,Guy Barnhart-Magen

SOC - cont...(09:00-17:59 PDT) - Chillout Lounge - Entertainment - Rusty,s1gnsof11fe,Pie & Darren,Merin

MC,Kampf,djdead

WS - CICD security: A new eldorado - Remi Escourrou,Gauthier Sebaux,Xavier Gerondeau

WS - Finding Security Vulnerabilities Through Fuzzing - Hardik Shah

WS - Introduction to Cryptographic Attacks - Matt Cheung

WS - The Art of Modern Malware Analysis: Initial Infection Malware, Infrastructure, and C2 Frameworks - Aaron Rosenmund,Ryan J Chapman,Josh Stroschein

WS - DFIR Against the Digital Darkness: An Intro to Forensicating Evil - Michael Register,Michael Solomon

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

---

- AIV - I'm not Keylogging you! Just some benign data collection for User Behavior Modeling - Harini Kannan
- ASV - cont...(09:00-16:59 PDT) - California CyberSecurity Institute Space Grand Challenge -
- ASV - cont...(10:00-16:59 PDT) - Hack the Airport with Intelligenesis -
- ASV - cont...(10:00-16:59 PDT) - Hack the Airfield with DDS -
- ASV - cont...(10:00-16:59 PDT) - Satellite Eavesdropping with DDS -
- ASV - cont...(10:00-15:59 PDT) - Red Balloon Failsat Challenges -
- ASV - cont...(10:00-11:59 PDT) - Pen Test Partners A320 Simulator -
- ASV - cont...(10:00-16:59 PDT) - Hack-A-Sat Digital Twin Workshop -
- ASV - cont...(10:00-16:59 PDT) - Amazon Web Services Aerospace and Satellite Jam -
- ASV - cont...(10:00-15:59 PDT) - Boeing ARINC 429 Airplane Challenge and CTF -
- ASV - That's No Moon -- A Look at the Space Threat Environment - Mike Campanelli
- ASV - (11:30-11:55 PDT) - DDS Space Signal Lab - James Pavur
- BHV - Where there's a kiosk, there's an escape - Michael Aguilar (v3ga)
- BHV - (11:30-11:59 PDT) - Department of Defense 5G Telemedicine and Medical Training: The Future of Healthcare the Remote Warrior - Paul Young
- BICV - Creating More Black Hackers: Growth Systems for Cybersecurity Enthusiasts - Segun Ebenezer Olaniyan
- BTV - cont...(10:30-11:30 PDT) - Obsidian Live: Eating the Elephant 1 byte at a Time - aviditas,ChocolateCoat
- BTV - cont...(10:30-11:30 PDT) - Obsidian Forensics: Kill Chain 1 Endpoint Forensics Walkthrough - Omenscan
- BTV - (11:30-12:30 PDT) - Obsidian: IR - It all starts here, scoping the incident - ChocolateCoat
- BTV - cont...(10:30-11:30 PDT) - Obsidian CTH: Go Phish: Visualizing Basic Malice - SamunoskeX
- BTV - (11:30-12:30 PDT) - Obsidian CTI: Generating Threat Intelligence from an Incident - Stephanie G.,l00sid,ttheveii0x
- BTV - Attribution and Bias: My terrible mistakes in threat intelligence attribution - Seongsu Park
- BTV - (11:45-12:45 PDT) - Malicious memory techniques on Windows and how to spot them - Connor Morley
- BTV - Practical Dark Web Hunting using Automated Scripts - Apurv Singh Gautam
- CLV - cont...(10:50-11:30 PDT) - Making the most of Microsoft cloud bug bounty programs: How I made in \$65,000 USD in bounties in 2021 - Nestori Syynimaa
- CLV - (11:30-12:10 PDT) - Flying Under Cloud Cover: Built-in Blind Spots in Cloud Security - Noam Dahan
- CPV - Positive Identification of Least Significant Bit Image Steganography - Michael Pelosi
- CPV - (11:30-11:59 PDT) - OPAQUE is Not Magic - Steve Thomas
- DC - The PACMAN Attack: Breaking PAC on the Apple M1 with Hardware Attacks - Joseph Ravichandran
- DC - cont...(10:30-11:15 PDT) - OopsSec -The bad, the worst and the ugly of APT's operations security - Tomer Bar
- DC - (11:30-11:50 PDT) - Running Rootkits Like A Nation-State Hacker - Omri Misgav
- DC - cont...(08:00-18:59 PDT) - Human Registration Open
- DC - The Dark Tangent & Mkfactor - Welcome to DEF CON & The Making of the DEF CON Badge - The Dark Tangent,Michael Whiteley (Mkfactor),Katie Whiteley (Mkfactor)
- DC - cont...(10:00-11:15 PDT) - Panel - DEF CON Policy Dept - What is it, and what are we trying to do for hackers in the policy world? - DEF CON Policy Dept
- DC - (11:30-12:15 PDT) - DEF CON Policy Dept - Special Edition Policy Talk - DEF CON Policy Dept
- DC - cont...(10:00-17:59 PDT) - Vendor Area Open
- DC - cont...(09:00-15:59 PDT) - Merch (formerly swag) Area Open -- README -
- DC - cont...(10:00-17:59 PDT) - Village Areas Open (Generally) -
- DDV - cont...(10:00-16:59 PDT) - DDV open and accepting drives for duplication -
- DL - cont...(10:00-11:55 PDT) - TheAllCommander - Matthew Handy
- DL - cont...(10:00-11:55 PDT) - Access Undenied on AWS - Noam Dahan
- DL - cont...(10:00-11:55 PDT) - Vajra - Your Weapon To Cloud - Raunak Parmar
- DL - cont...(10:00-11:55 PDT) - FISSURE: The RF Framework - Christopher Poore
- DL - cont...(10:00-11:55 PDT) - Zuthaka: A Command & Controls (C2s) integration framework - Lucas Bonastre,Alberto Herrera
- HHV - cont...(10:00-17:59 PDT) - Solder Skills Village - Open
- HHV - cont...(10:00-17:59 PDT) - Hardware Hacking Village - Open
- HHV - From Zero To Sao ... Or, How Far Does This Rabbit Hole Go? - Bradán Lane

HRV - (11:30-12:30 PDT) - [Your Amateur Radio License and You](#) - Justin/InkRF  
IOTV - cont...(10:00-17:59 PDT) - [Hands on Hardware Hacking – eMMC to Root](#) - Deral Heiland  
IOTV - cont...(10:00-17:59 PDT) - [Drone Hack](#) -  
IOTV - cont...(10:00-17:59 PDT) - [IoT Village CTF](#) -  
IOTV - cont...(10:00-17:59 PDT) - [IoT Village CTF Challenges](#) -  
IOTV - cont...(10:00-17:59 PDT) - [Hands on hacking labs](#) -  
IOTV - [Hacking Product Security Interviews](#) -  
IOTV - (11:30-11:59 PDT) - [Hacking Product Security Interviews](#) -  
LPV - [Medeco cam lock exploit "an old attack made new again"](#) - N thing  
MIV - cont...(10:00-11:30 PDT) - [The hybrid strategies of autocratic states: narrative characteristics of disinformation campaigns in relation to issues of a scientific-health nature](#) - Carlos Galán  
MIV - (11:30-13:30 PDT) - [Dazed and Seriously Confused: Analysis of Data Voids & the Disinformation Landscape of Central Asia](#) - Rhyner Washburn  
MIV - (11:30-13:30 PDT) - [Detecting the "Fake News" Before It Was Even Written, Media Literacy, and Flattening the Curve of the COVID-19 Infodemic](#) - Preslav Nakov  
MIV - (11:30-13:30 PDT) - [Examining the urgency of gendered health misinformation online through three case studies](#) - Jenna Sherman  
MIV - (11:30-13:30 PDT) - [Cognitive Security: Human Vulnerabilities, Exploits, & TTPs](#) - Matthew Canham  
MIV - (11:30-13:30 PDT) - [SimPPL: Simulating Social Networks and Disinformation](#) - Swapneel Mehta  
MIV - (11:30-13:30 PDT) - [Uncovering multi-platform misinformation campaigns with Information Tracer](#) - Zhouhan Chen  
RHV - [Rock the Cash Box](#) - Spicy Wasabi  
SKY - cont...(10:35-11:25 PDT) - [Hundreds of incidents, what can we share?](#) - Brenton Morris,Guy Barnhart-Magen  
SKY - (11:40-11:59 PDT) - [Android, Birthday Cake, Open Wifi... Oh my!](#) - A.Krontab  
SOC - cont...(09:00-17:59 PDT) - [Chillout Lounge - Entertainment](#) - Rusty,s1gnsof1ife,Pie & Darren,Merin  
MC,Kampf,djdead  
SOC - No Starch Press - Book Signing - Craig Smith, The Car Hacker's Handbook  
WS - cont...(10:00-13:59 PDT) - [CICD security: A new eldorado](#) - Remi Escourrou,Gauthier Sebaux,Xavier Gerondeau  
WS - cont...(10:00-13:59 PDT) - [Finding Security Vulnerabilities Through Fuzzing](#) - Hardik Shah  
WS - cont...(10:00-13:59 PDT) - [Introduction to Cryptographic Attacks](#) - Matt Cheung  
WS - cont...(10:00-13:59 PDT) - [The Art of Modern Malware Analysis: Initial Infection Malware, Infrastructure, and C2 Frameworks](#) - Aaron Rosenmund,Ryan J Chapman,Josh Stroschein  
WS - cont...(10:00-13:59 PDT) - [DFIR Against the Digital Darkness: An Intro to Forensicking Evil](#) - Michael Register,Michael Solomon

## Friday - 12:00 PDT

---

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

---

AIV - [AI Village Keynote](#) - Keith E. Sonderling  
ASV - cont...(09:00-16:59 PDT) - [California CyberSecurity Institute Space Grand Challenge](#) -  
ASV - cont...(10:00-16:59 PDT) - [Hack the Airport with Intelligenesis](#) -  
ASV - cont...(10:00-16:59 PDT) - [Hack the Airfield with DDS](#) -  
ASV - cont...(10:00-16:59 PDT) - [Satellite Eavesdropping with DDS](#) -  
ASV - cont...(10:00-15:59 PDT) - [Red Balloon Failsat Challenges](#) -  
ASV - cont...(10:00-16:59 PDT) - [Hack-A-Sat Digital Twin Workshop](#) -  
ASV - cont...(10:00-16:59 PDT) - [Amazon Web Services Aerospace and Satellite Jam](#) -  
ASV - cont...(10:00-15:59 PDT) - [Boeing ARINC 429 Airplane Challenge and CTF](#) -  
ASV - [Hackers Help Make My Airline Secure](#) - Deneen Defiore  
ASV - [Hack-A-Sat Aerospace PiSat Challenge](#) -  
BHV - [Gird your loins: premise and perils of biomanufacturing](#) - Nathan Case  
BHV - (12:30-13:30 PDT) - [How to stop Surveillance Capitalism in Healthcare](#) - Andrea Downing,Jillian Simons,Valencia Robinson  
BICV - ["The Man" in the Middle](#) - Alexis Hancock  
BTW - cont...(11:30-12:30 PDT) - [Obsidian: IR - It all starts here, scoping the incident](#) - ChocolateCoat  
BTW - cont...(11:30-12:30 PDT) - [Obsidian CTI: Generating Threat Intelligence from an Incident](#) - Stephanie

G.,l00sid,ttheveii0x

**BTV** - cont...(11:45-12:45 PDT) - Malicious memory techniques on Windows and how to spot them - Connor Morley

**BTV** - cont...(11:00-12:30 PDT) - Practical Dark Web Hunting using Automated Scripts - Apurv Singh Gautam

**CLV** - cont...(11:30-12:10 PDT) - Flying Under Cloud Cover: Built-in Blind Spots in Cloud Security - Noam Dahan

**CLV** - A ransomware actor looks at the clouds: attacking in a cloud-native way - Jay Chen

**CLV** - (12:30-13:10 PDT) - Weather Proofing GCP Defaults - Shannon McHale

**CPV** - PSA: Doorbell Cameras Have Mics, Too - Yael Grauer,Matthew Guariglia

**DC** - Avoiding Memory Scanners: Customizing Malware to Evade YARA, PE-sieve, and More - Kyle Avery

**DC** - One Bootloader to Load Them All - Jesse Michael,Mickey Shkatov

**DC** - cont...(08:00-18:59 PDT) - Human Registration Open

**DC** - Glitched on Earth by humans: A Black-Box Security Evaluation of the SpaceX Starlink User Terminal - Lennert Wouters

**DC** - cont...(11:30-12:15 PDT) - DEF CON Policy Dept - Special Edition Policy Talk - DEF CON Policy Dept

**DC** - (12:30-13:15 PDT) - DEF CON Policy Dept - Special Edition Policy Talk - DEF CON Policy Dept

**DC** - cont...(10:00-17:59 PDT) - Vendor Area Open

**DC** - cont...(09:00-15:59 PDT) - Merch (formerly swag) Area Open -- README -

**DC** - cont...(10:00-17:59 PDT) - Village Areas Open (Generally) -

**DDV** - cont...(10:00-16:59 PDT) - DDV open and accepting drives for duplication -

**DL** - Packet Sender - Dan Nagle

**DL** - Wakanda Land - Stephen Kofi Asamoah

**DL** - AzureGoat: Damn Vulnerable Azure Infrastructure - Rachna Umraniya,Nishant Sharma

**DL** - EMBA - Open-Source Firmware Security Testing - Pascal Eckmann,Michael Messner

**DL** - Mercury - David McGrew,Brandon Enright

**HHV** - cont...(10:00-17:59 PDT) - Solder Skills Village - Open

**HHV** - cont...(10:00-17:59 PDT) - Hardware Hacking Village - Open

**HRV** - cont...(11:30-12:30 PDT) - Your Amateur Radio License and You - Justin/InkRF

**IOTV** - cont...(10:00-17:59 PDT) - Hands on Hardware Hacking – eMMC to Root - Deral Heiland

**IOTV** - cont...(10:00-17:59 PDT) - Drone Hack -

**IOTV** - cont...(10:00-17:59 PDT) - IoT Village CTF -

**IOTV** - cont...(10:00-17:59 PDT) - IoT Village CTF Challenges -

**IOTV** - cont...(10:00-17:59 PDT) - Hands on hacking labs -

**LPV** - The least secure biometric lock on Earth? - Seth Kintigh

**MIV** - cont...(11:30-13:30 PDT) - Dazed and Seriously Confused: Analysis of Data Voids & the Disinformation Landscape of Central Asia - Rhyner Washburn

**MIV** - cont...(11:30-13:30 PDT) - Detecting the "Fake News" Before It Was Even Written, Media Literacy, and Flattening the Curve of the COVID-19 Infodemic - Preslav Nakov

**MIV** - cont...(11:30-13:30 PDT) - Examining the urgency of gendered health misinformation online through three case studies - Jenna Sherman

**MIV** - cont...(11:30-13:30 PDT) - Cognitive Security: Human Vulnerabilities, Exploits, & TTPs - Matthew Canham

**MIV** - cont...(11:30-13:30 PDT) - SimPPL: Simulating Social Networks and Disinformation - Swapneel Mehta

**MIV** - cont...(11:30-13:30 PDT) - Uncovering multi-platform misinformation campaigns with Information Tracer - Zhouhan Chen

**PLV** - Hacking law is for hackers - how recent changes to CFAA, DMCA, and global policies affect security research - Leonard Bailey,Harley Geiger

**SKY** - The Richest Phisherman in Colombia - Matt Mosley,Nick Ascoli

**SKY** - (12:45-13:35 PDT) - Taking Down the Grid - Joe Slowik

**SOC** - cont...(09:00-17:59 PDT) - Chillout Lounge - Entertainment - Rusty,s1gns0fl1fe,Pie & Darren,Merin

MC,Kampf,djdead

**SOC** - No Starch Press - Book Signing - Jasper van Woudenberg, Hardware Hacking Handbook

**SOC** - Friends of Bill W -

**WS** - cont...(10:00-13:59 PDT) - CICD security: A new eldorado - Remi Escourrou,Gauthier Sebaux,Xavier Gerondeau

**WS** - cont...(10:00-13:59 PDT) - Finding Security Vulnerabilities Through Fuzzing - Hardik Shah

**WS** - cont...(10:00-13:59 PDT) - Introduction to Cryptographic Attacks - Matt Cheung

**WS** - cont...(10:00-13:59 PDT) - The Art of Modern Malware Analysis: Initial Infection Malware, Infrastructure, and C2 Frameworks - Aaron Rosenmund,Ryan J Chapman,Josh Stroschein

## Friday - 13:00 PDT

---

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

AIV - Machine Learning Security Evasion Competition Launch - Hyrum Anderson

ASV - cont...(09:00-16:59 PDT) - California CyberSecurity Institute Space Grand Challenge -

ASV - cont...(10:00-16:59 PDT) - Hack the Airport with Intelligenesis -

ASV - cont...(10:00-16:59 PDT) - Hack the Airfield with DDS -

ASV - cont...(10:00-16:59 PDT) - Satellite Eavesdropping with DDS -

ASV - cont...(10:00-15:59 PDT) - Red Balloon Failsat Challenges -

ASV - cont...(10:00-16:59 PDT) - Hack-A-Sat Digital Twin Workshop -

ASV - cont...(10:00-16:59 PDT) - Amazon Web Services Aerospace and Satellite Jam -

ASV - cont...(10:00-15:59 PDT) - Boeing ARINC 429 Airplane Challenge and CTF -

ASV - cont...(12:00-16:59 PDT) - Hack-A-Sat Aerospace PiSat Challenge -

ASV - Resumé Review and Career Guidance Session -

ASV - Cyber Star Card Game Tutorial - Rick White

ASV - Cyber Star© Competition Presented by The Space ISAC -

ASV - Pen Test Partners A320 Simulator -

ASV - (13:30-13:55 PDT) - Securing the Future of Aviation CyberSecurity - Timothy Weston

BHV - cont...(12:30-13:30 PDT) - How to stop Surveillance Capitalism in Healthcare - Andrea Downing,Jillian Simons,Valencia Robinson

BHV - (13:30-13:59 PDT) - DIY Medicine With Unusual Uses for Existing FDA-Approved Drugs - Mixæl S. Laufer

BTW - Obsidian Forensics: KillChain1 - Adventures in Splunk and Security Onion - ExtremePaperClip,Omenscan,Wes Lambert

BTW - Obsidian: IR - Mise En Place for Investigations - aviditas,ChocolateCoat,CountZ3r0

BTW - Obsidian CTH: Hunting for Adversary's Schedule - Cyb3rHawk

BTW - Improving security posture of MacOS and Linux with Azure AD - Michael Epping,Mark Morowczynski

BTW - Ransomware ATT&CK and Defense - Ronny Thammasathiti,Daniel Chen,Esther Matut,Ben Hughes,Nick Baker

CLV - cont...(12:30-13:10 PDT) - Weather Proofing GCP Defaults - Shannon McHale

CLV - Security at Every Step: The TL;DR on Securing Your AWS Code Pipeline - Cassandra Young (muteki)

CLV - (13:40-14:20 PDT) - Sponsored Talk

CPV - Reflections on 9 Years of CPV - Whitney Merrill

CPV - (13:30-13:59 PDT) - How to Respond to Data Subject Access Requests - Irene Mo

DC - Backdooring Pickles: A decade only made things worse - ColdwaterQ

DC - (13:30-13:50 PDT) - Weaponizing Windows Syscalls as Modern, 32-bit Shellcode - Tarek Abdelmotaleb,Dr. Bramwell Brizendine

DC - You're <strike>Muted</strike>Rooted - Patrick Wardle

DC - cont...(08:00-18:59 PDT) - Human Registration Open

DC - Emoji Shellcoding: , , and - Georges-Axel Jaloyan,Hadrien Barral

DC - cont...(12:30-13:15 PDT) - DEF CON Policy Dept - Special Edition Policy Talk - DEF CON Policy Dept

DC - (13:30-14:15 PDT) - DEF CON Policy Dept - Special Edition Policy Talk - DEF CON Policy Dept

DC - cont...(10:00-17:59 PDT) - Vendor Area Open

DC - cont...(09:00-15:59 PDT) - Merch (formerly swag) Area Open -- README -

DC - cont...(10:00-17:59 PDT) - Village Areas Open (Generally) -

DDV - cont...(10:00-16:59 PDT) - DDV open and accepting drives for duplication -

DDV - How long do hard drives and SSDs live, and what can they tell us along the way? - Andrew Klein

DL - cont...(12:00-13:55 PDT) - Packet Sender - Dan Nagle

DL - cont...(12:00-13:55 PDT) - Wakanda Land - Stephen Kofi Asamoah

DL - cont...(12:00-13:55 PDT) - AzureGoat: Damn Vulnerable Azure Infrastructure - Rachna Umriani,Nishant Sharma

DL - cont...(12:00-13:55 PDT) - EMBA - Open-Source Firmware Security Testing - Pascal Eckmann,Michael Messner

DL - cont...(12:00-13:55 PDT) - Mercury - David McGrew,Brandon Enright

HHV - cont...(10:00-17:59 PDT) - Solder Skills Village - Open

HHV - cont...(10:00-17:59 PDT) - Hardware Hacking Village - Open  
HHV - Reversing An M32C Firmware – Lesson Learned From Playing With An Uncommon Architecture - Philippe Laulheret  
HRV - Free Amateur Radio License Exams -  
IOTV - cont...(10:00-17:59 PDT) - Hands on Hardware Hacking – eMMC to Root - Deral Heiland  
IOTV - cont...(10:00-17:59 PDT) - Drone Hack -  
IOTV - cont...(10:00-17:59 PDT) - IoT Village CTF -  
IOTV - cont...(10:00-17:59 PDT) - IoT Village CTF Challenges -  
IOTV - cont...(10:00-17:59 PDT) - Hands on hacking labs -  
LPV - Intro to Lockpicking - TOOOL  
MIV - cont...(11:30-13:30 PDT) - Dazed and Seriously Confused: Analysis of Data Voids & the Disinformation Landscape of Central Asia - Rhyner Washburn  
MIV - cont...(11:30-13:30 PDT) - Detecting the "Fake News" Before It Was Even Written, Media Literacy, and Flattening the Curve of the COVID-19 Infodemic - Preslav Nakov  
MIV - cont...(11:30-13:30 PDT) - Examining the urgency of gendered health misinformation online through three case studies - Jenna Sherman  
MIV - cont...(11:30-13:30 PDT) - Cognitive Security: Human Vulnerabilities, Exploits, & TTPs - Matthew Canham  
MIV - cont...(11:30-13:30 PDT) - SimPPL: Simulating Social Networks and Disinformation - Swapneel Mehta  
MIV - cont...(11:30-13:30 PDT) - Uncovering multi-platform misinformation campaigns with Information Tracer - Zhouhan Chen  
PLV - cont...(12:00-13:45 PDT) - Hacking law is for hackers - how recent changes to CFAA, DMCA, and global policies affect security research - Leonard Bailey, Harley Geiger  
PWV - Hacking Hashcat - Ray "Senpai" Morris  
SKY - cont...(12:45-13:35 PDT) - Taking Down the Grid - Joe Slowik  
SKY - (13:50-14:40 PDT) - Don't Blow A Fuse: Some Truths about Fusion Centres - 3ncr1pt3d  
SOC - cont...(09:00-17:59 PDT) - Chillout Lounge - Entertainment - Rusty,s1gnsof11fe,Pie & Darren,Merin  
MC,Kampf,djdead  
SOC - No Starch Press - Book Signing - Fotios Chantzis, Paulino Calderon, & Beau Woods, Practical IoT Hacking  
WS - cont...(10:00-13:59 PDT) - CICD security: A new eldorado - Remi Escourrou, Gauthier Sebaux, Xavier Gerondeau  
WS - cont...(10:00-13:59 PDT) - Finding Security Vulnerabilities Through Fuzzing - Hardik Shah  
WS - cont...(10:00-13:59 PDT) - Introduction to Cryptographic Attacks - Matt Cheung  
WS - cont...(10:00-13:59 PDT) - The Art of Modern Malware Analysis: Initial Infection Malware, Infrastructure, and C2 Frameworks - Aaron Rosenmund, Ryan J Chapman, Josh Stroschein  
WS - cont...(10:00-13:59 PDT) - DFIR Against the Digital Darkness: An Intro to Forensinating Evil - Michael Register, Michael Solomon

## Friday - 14:00 PDT

---

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

---

AIV - The Chaos of Coding with Language Models - Nick Dorion  
ASV - cont...(09:00-16:59 PDT) - California CyberSecurity Institute Space Grand Challenge -  
ASV - cont...(10:00-16:59 PDT) - Hack the Airport with Intelligenesis -  
ASV - cont...(10:00-16:59 PDT) - Hack the Airfield with DDS -  
ASV - cont...(10:00-16:59 PDT) - Satellite Eavesdropping with DDS -  
ASV - cont...(10:00-15:59 PDT) - Red Balloon Failsat Challenges -  
ASV - cont...(10:00-16:59 PDT) - Hack-A-Sat Digital Twin Workshop -  
ASV - cont...(10:00-16:59 PDT) - Amazon Web Services Aerospace and Satellite Jam -  
ASV - cont...(10:00-15:59 PDT) - Boeing ARINC 429 Airplane Challenge and CTF -  
ASV - cont...(12:00-16:59 PDT) - Hack-A-Sat Aerospace PiSat Challenge -  
ASV - cont...(13:00-14:59 PDT) - Resumé Review and Career Guidance Session -  
ASV - cont...(13:00-14:59 PDT) - Pen Test Partners A320 Simulator -  
ASV - Final Boarding Call for Cyber Policy Airlines Flight 443 - Rebecca Ash, Ayan Islam, Mary Brooks, Olivia Stella  
BHV - (14:30-15:59 PDT) - DIY MQTT IoT (or how you can turn your home into an interconnected palace of human-centric data) - Cody Wayne Burkhardt  
BICV - DEI in Cybersecurity (Breaking through the barrier, behind the barrier... behind the barrier) - Damian Grant

[BTV - Obsidian CTH Live: Killchain 1 Walkthrough](#) -

[BTV - Obsidian Forensics: The Importance of Sysmon for Investigations](#) - ExtremePaperClip

[BTV - Obsidian REM: Long Walks On The Beach: Analyzing Collected PowerShells](#) - Alison N

[BTV - \(14:15-15:15 PDT\) - Lend me your IR's!](#) - Matt Scheurer

[BTV - cont...\(13:00-14:30 PDT\) - Ransomware ATT&CK and Defense](#) - Ronny Thammasathiti,Daniel Chen,Esther Matut,Ben Hughes,Nick Baker

[CLV - cont...\(13:40-14:20 PDT\) - Sponsored Talk](#)

[CLV - \(14:20-14:50 PDT\) - Shopping for Vulnerabilities - How Cloud Service Provider Marketplaces can Help White and Black Hat Vulnerability Research](#) - Alexandre Sieira

[CPV - Securing and Standardizing Data Rights Requests with a Data Rights Protocol](#) - Ginny Fahs,Ryan Rix,Dazza Greenwood

[CPV - \(14:30-14:59 PDT\) - The Multiverse of Madness: Navigating the 50-State Approach to Privacy and Security](#) - Anthony Hendricks

[DC - Process injection: breaking all macOS security layers with a single vulnerability](#) - Thijs Alkemade

[DC - Phreaking 2.0 - Abusing Microsoft Teams Direct Routing](#) - Moritz Abrell

[DC - \(14:30-15:15 PDT\) - Trace me if you can: Bypassing Linux Syscall Tracing](#) - Rex Guo,Junyuan Zeng

[DC - cont...\(08:00-18:59 PDT\) - Human Registration Open](#)

[DC - Space Jam: Exploring Radio Frequency Attacks in Outer Space](#) - James Pavur

[DC - cont...\(13:30-14:15 PDT\) - DEF CON Policy Dept - Special Edition Policy Talk](#) - DEF CON Policy Dept

[DC - \(14:30-15:15 PDT\) - Leak The Planet: Veritatem cognoscere non pereat mundus](#) - Xan North,Emma Best

[DC - cont...\(10:00-17:59 PDT\) - Vendor Area Open](#)

[DC - cont...\(09:00-15:59 PDT\) - Merch \(formerly swag\) Area Open -- README](#) -

[DC - cont...\(10:00-17:59 PDT\) - Village Areas Open \(Generally\)](#) -

[DDV - cont...\(10:00-16:59 PDT\) - DDV open and accepting drives for duplication](#) -

[DL - CyberPeace Builders](#) - Adrien Ogee

[DL - AWSGoat : A Damn Vulnerable AWS Infrastructure](#) - Sanjeev Mahunta,Jeswin Mathai

[DL - AADInternals: The Ultimate Azure AD Hacking Toolkit](#) - Nestori Syynimaa

[DL - PCILeech and MemProcFS](#) - Ian Vitek,Ulf Frisk

[DL - Badrats: Initial Access Made Easy](#) - Kevin Clark,Dominic "Cryillic" Cunningham

[HHV - cont...\(10:00-17:59 PDT\) - Solder Skills Village](#) - Open

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

[HHV - Movie-Style Hardware Hacking](#) - Bryan C. Geraghty

[HRV - cont...\(13:00-15:59 PDT\) - Free Amateur Radio License Exams](#) -

[IOTV - cont...\(10:00-17:59 PDT\) - Hands on Hardware Hacking – eMMC to Root](#) - Deral Heiland

[IOTV - cont...\(10:00-17:59 PDT\) - Drone Hack](#) -

[IOTV - cont...\(10:00-17:59 PDT\) - IoT Village CTF](#) -

[IOTV - cont...\(10:00-17:59 PDT\) - IoT Village CTF Challenges](#) -

[IOTV - cont...\(10:00-17:59 PDT\) - Hands on hacking labs](#) -

[LPV - The Right Way To Do Wrong: Physical security secrets of criminals and professionals alike](#) - Patrick McNeil

[MIV - \(14:30-15:59 PDT\) - Fireside Chat](#) - Adam Hickey,Jennifer Mathieu

[MIV - \(14:30-15:59 PDT\) - FARA and DOJ's Approach to Disinformation](#) - Adam Hickey

[MIV - \(14:30-15:59 PDT\) - Multi-Stakeholder Online Harm Threat Analysis](#) - Jennifer Mathieu

[PLV - Defense Through a TAC \(Technical Advisory Committee\)](#) - The Dark Tangent

[SKY - cont...\(13:50-14:40 PDT\) - Don't Blow A Fuse: Some Truths about Fusion Centres](#) - 3ncr1pt3d

[SKY - \(14:55-15:45 PDT\) - Cloud Threat Actors: No longer cryptojacking for fun and profit](#) - Nathaniel Quist

[SOC - cont...\(09:00-17:59 PDT\) - Chillout Lounge - Entertainment](#) - Rusty,s1gnsof1fe,Pie & Darren,Merin

[MC,Kampf,djdead](#)

[SOC - No Starch Press - Book Signing](#) - Travis Goodspeed, PoC or GTFO Volume 3

## Friday - 15:00 PDT

---

[Return to Index - Locations Legend](#)

---

[AIV - LATMA - Lateral movement analyzer](#) - Gal Sadeh

[ASV - cont...\(09:00-16:59 PDT\) - California CyberSecurity Institute Space Grand Challenge](#) -

ASV - cont...(10:00-16:59 PDT) - Hack the Airport with Intelligenesis -  
ASV - cont...(10:00-16:59 PDT) - Hack the Airfield with DDS -  
ASV - cont...(10:00-16:59 PDT) - Satellite Eavesdropping with DDS -  
ASV - cont...(10:00-15:59 PDT) - Red Balloon Failsat Challenges -  
ASV - cont...(10:00-16:59 PDT) - Hack-A-Sat Digital Twin Workshop -  
ASV - cont...(10:00-16:59 PDT) - Amazon Web Services Aerospace and Satellite Jam -  
ASV - cont...(10:00-15:59 PDT) - Boeing ARINC 429 Airplane Challenge and CTF -  
ASV - cont...(12:00-16:59 PDT) - Hack-A-Sat Aerospace PiSat Challenge -  
ASV - Ask an Airport CISO - Aakinn Patel  
BHV - cont...(14:30-15:59 PDT) - DIY MQTT IoT (or how you can turn your home into an interconnected palace of human-centric data) - Cody Wayne Burkhart  
BTV - Heavyweights: Threat Hunting at Scale - Sherrod DeGrippo,Ashlee Benge,Jamie Williams,nohackme,Sean Zadig,Ryan Kovar  
BTV - cont...(14:15-15:15 PDT) - Lend me your IR's! - Matt Scheurer  
BTV - (15:30-16:30 PDT) - Malware Hunting - Discovering techniques in PDF malicious - Filipi Pires  
CLV - Prowler Open Source Cloud Security: A Deep Dive Workshop - Toni de la Fuente  
CPV - ID theft insurance - The Emperor's new clothes? - Per Thorsheim  
DC - LSASS Shtinkering: Abusing Windows Error Reporting to Dump LSASS - Asaf Gilboa,Ron Ben Yitzhak  
DC - cont...(14:30-15:15 PDT) - Trace me if you can: Bypassing Linux Syscall Tracing - Rex Guo,Junyuan Zeng  
DC - (15:30-16:15 PDT) - Browser-Powered Desync Attacks: A New Frontier in HTTP Request Smuggling - James Kettle  
DC - cont...(08:00-18:59 PDT) - Human Registration Open  
DC - Exploring the hidden attack surface of OEM IoT devices: pwnning thousands of routers with a vulnerability in Realtek's SDK for eCos OS. - Octavio Galland,Octavio Gianatiempo  
DC - cont...(14:30-15:15 PDT) - Leak The Planet: Veritatem cognoscere non pereat mundus - Xan North,Emma Best  
DC - (15:30-16:15 PDT) - How Russia is trying to block Tor - Roger Dingledine  
DC - cont...(10:00-17:59 PDT) - Vendor Area Open  
DC - cont...(09:00-15:59 PDT) - Merch (formerly swag) Area Open -- README -  
DC - cont...(10:00-17:59 PDT) - Village Areas Open (Generally) -  
DDV - cont...(10:00-16:59 PDT) - DDV open and accepting drives for duplication -  
DDV - No bricks without clay - Data Fusion and Duplication in Cybersecurity - Lior Kolnik  
DL - cont...(14:00-15:55 PDT) - CyberPeace Builders - Adrien Ogee  
DL - cont...(14:00-15:55 PDT) - AWSGoat : A Damn Vulnerable AWS Infrastructure - Sanjeev Mahunta,Jeswin Mathai  
DL - cont...(14:00-15:55 PDT) - AADInternals: The Ultimate Azure AD Hacking Toolkit - Nestori Syynimaa  
DL - cont...(14:00-15:55 PDT) - PCILeech and MemProcFS - Ian Vitek,Ulf Frisk  
DL - cont...(14:00-15:55 PDT) - Badrats: Initial Access Made Easy - Kevin Clark,Dominic "Cryillic" Cunningham  
HHV - cont...(10:00-17:59 PDT) - Solder Skills Village - Open  
HHV - cont...(10:00-17:59 PDT) - Hardware Hacking Village - Open  
HHV - Injectyll-Hide: Build-Your-Own Hardware Implants - Jeremy Miller,Jonathan Fischer  
HRV - cont...(13:00-15:59 PDT) - Free Amateur Radio License Exams -  
HRV - Hacking Ham Radio: Dropping Shells at 1200 Baud - Rick Osgood  
IOTV - cont...(10:00-17:59 PDT) - Hands on Hardware Hacking – eMMC to Root - Deral Heiland  
IOTV - cont...(10:00-17:59 PDT) - Drone Hack -  
IOTV - cont...(10:00-17:59 PDT) - IoT Village CTF -  
IOTV - cont...(10:00-17:59 PDT) - IoT Village CTF Challenges -  
IOTV - cont...(10:00-17:59 PDT) - Hands on hacking labs -  
LPV - (15:30-15:45 PDT) - Handcuffs and how they work - Steven Collins  
MIV - cont...(14:30-15:59 PDT) - Fireside Chat - Adam Hickey,Jennifer Mathieu  
MIV - cont...(14:30-15:59 PDT) - FARA and DOJ's Approach to Disinformation - Adam Hickey  
MIV - cont...(14:30-15:59 PDT) - Multi-Stakeholder Online Harm Threat Analysis - Jennifer Mathieu  
PLV - cont...(14:00-15:45 PDT) - Defense Through a TAC (Technical Advisory Committee) - The Dark Tangent  
RHV - Mitigating vulnerabilities in two-factor authentication in preventing account takeover - Larsbodian  
SKY - cont...(14:55-15:45 PDT) - Cloud Threat Actors: No longer cryptojacking for fun and profit - Nathaniel Quist  
SOC - cont...(09:00-17:59 PDT) - Chillout Lounge - Entertainment - Rusty,s1gnsof11fe,Pie & Darren,Merin  
MC,Kampf,djdead  
SOC - (15:30-16:30 PDT) - EFF: Reproductive Justice in the Age of Surveillance -

WS - Hacking the Metal 2: Hardware and the Evolution of C Creatures - Eigentourist  
WS - Hand On Mainframe Buffer Overflows - RCE Edition - Phil Young,Jake Labelle  
WS - Securing Industrial Control Systems from the core: PLC secure coding practices - Arnaud Soullie,Alexandrine Torrents  
WS - FROM ZERO TO HERO IN A BLOCKCHAIN SECURITY - Roman Zaikin,Dikla Barda,Oded Vanunu  
WS - Securing Smart Contracts - Irvin Lemus,Kaitlyn Handleman,Elizabeth Biddlecome,Sam Bowne

## Friday - 16:00 PDT

---

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

---

AIV - Panel: AI and Hiring Tech  
ASV - cont...(09:00-16:59 PDT) - California CyberSecurity Institute Space Grand Challenge -  
ASV - cont...(10:00-16:59 PDT) - Hack the Airport with Intelligenesis -  
ASV - cont...(10:00-16:59 PDT) - Hack the Airfield with DDS -  
ASV - cont...(10:00-16:59 PDT) - Satellite Eavesdropping with DDS -  
ASV - cont...(10:00-16:59 PDT) - Hack-A-Sat Digital Twin Workshop -  
ASV - cont...(10:00-16:59 PDT) - Amazon Web Services Aerospace and Satellite Jam -  
ASV - cont...(12:00-16:59 PDT) - Hack-A-Sat Aerospace PiSat Challenge -  
ASV - Pen Test Partner Power Hour - Ken Munro,Alex Lomas  
BHV - (16:30-17:59 PDT) - Medical Device Hacking: A hands on introduction - Malcolm Galland  
BICV - The Last Log4Shell Talk You Need - Ochuan Marshall  
BTV - Take Your Security Skills From Good to Better to Best! - Ricky Banda,Neumann Lim (scsideath),Tracy Z. Maleeff,Kimberly Mentzell,Tanisha O'Donoghue  
BTV - cont...(15:30-16:30 PDT) - Malware Hunting - Discovering techniques in PDF malicious - Filipi Pires  
BTV - (16:45-16:59 PDT) - YARA Rules to Rule them All - Saurabh Chaudhary  
CLV - cont...(15:00-16:59 PDT) - Prowler Open Source Cloud Security: A Deep Dive Workshop - Toni de la Fuente  
CPV - Once More Unto the Breach: Federal Regulators' Response to Privacy Breaches and Consumer Harms - Erie Meyer,Alexis Goldstein  
CPV - (16:45-17:30 PDT) - Owned or pwned? No peakin' or tweakin'! - Nick Vidal,Richard Zak  
DC - Wireless Keystroke Injection (WKI) via Bluetooth Low Energy (BLE) - Fernando Perera,Jose Pico  
DC - cont...(15:30-16:15 PDT) - Browser-Powered Desync Attacks: A New Frontier in HTTP Request Smuggling - James Kettle  
DC - (16:30-17:15 PDT) - A dead man's full-yet-responsible-disclosure system - Yolan Romailler  
DC - cont...(08:00-18:59 PDT) - Human Registration Open  
DC - Hacking ISPs with Point-to-Pwn Protocol over Ethernet (PPPoE) - Gal Zror  
DC - cont...(15:30-16:15 PDT) - How Russia is trying to block Tor - Roger Dingledine  
DC - (16:30-17:15 PDT) - DEF CON Policy Dept - Special Edition Policy Talk - DEF CON Policy Dept  
DC - cont...(10:00-17:59 PDT) - Vendor Area Open  
DC - cont...(10:00-17:59 PDT) - Village Areas Open (Generally) -  
DDV - cont...(10:00-16:59 PDT) - DDV open and accepting drives for duplication -  
HHV - cont...(10:00-17:59 PDT) - Solder Skills Village - Open  
HHV - cont...(10:00-17:59 PDT) - Hardware Hacking Village - Open  
IOTV - cont...(10:00-17:59 PDT) - Hands on Hardware Hacking – eMMC to Root - Deral Heiland  
IOTV - cont...(10:00-17:59 PDT) - Drone Hack -  
IOTV - cont...(10:00-17:59 PDT) - IoT Village CTF -  
IOTV - cont...(10:00-17:59 PDT) - IoT Village CTF Challenges -  
IOTV - cont...(10:00-17:59 PDT) - Hands on hacking labs -  
LPV - Intro to Lockpicking - TOOOL  
MIV - History of the weaponization of social media - Gina Rosenthal  
MIV - Tracking Scams and Disinformation by Hacking Link Shorteners - Justin Rhinehart,Sam Curry  
MIV - History of Russian Cyber & Information Warfare (2007-Present) - Ryan Westman  
MIV - Information Confrontation 2022 - A loud war and a quiet enemy - Luke Richards  
PLV - Election Security Bridge Building - Jack Cable,Trevor Timmons,Michael Ross  
PLV - Moving Regulation Upstream - An Increasing focus on the Role of Digital Service Providers - Jen Ellis,Irfan Hemanji,Adam Dobell

[SKY - Automated Trolling for Fun and No Profit](#) - burninator

[SOC - cont...\(09:00-17:59 PDT\) - Chillout Lounge - Entertainment](#) - Rusty,s1gns0f1fe,Pie & Darren,Merin MC,Kampf,djdead

[SOC - Queercon Mixer](#) -

[SOC - cont...\(15:30-16:30 PDT\) - EFF: Reproductive Justice in the Age of Surveillance](#) -

[SOC - DC404/DC678/DC770/DC470 \(Atlanta Metro\) Meetup](#) -

[SOC - DEF CON Holland DC3115 & DC3120 Group Meetup](#) -

[WS - cont...\(15:00-18:59 PDT\) - Hacking the Metal 2: Hardware and the Evolution of C Creatures](#) - Eigentourist

[WS - cont...\(15:00-18:59 PDT\) - Hand On Mainframe Buffer Overflows - RCE Edition](#) - Phil Young,Jake Labelle

[WS - cont...\(15:00-18:59 PDT\) - Securing Industrial Control Systems from the core: PLC secure coding practices](#) - Arnaud Soullie,Alexandrine Torrents

[WS - cont...\(15:00-18:59 PDT\) - FROM ZERO TO HERO IN A BLOCKCHAIN SECURITY](#) - Roman Zaikin,Dikla Barda,Oded Vanunu

[WS - cont...\(15:00-18:59 PDT\) - Securing Smart Contracts](#) - Irvin Lemus,Kaitlyn Handleman,Elizabeth Biddlecome,Sam Bowne

## Friday - 17:00 PDT

---

[Return to Index - Locations Legend](#)

---

[BHV - cont...\(16:30-17:59 PDT\) - Medical Device Hacking: A hands on introduction](#) - Malcolm Galland

[BTV - Blue Teaming Cloud: Security Engineering for Cloud Forensics & Incident Response](#) - KyleHaxWhy,Cassandra Young (muteki),MissTech,John Orleans

[CPV - cont...\(16:45-17:30 PDT\) - Owned or pwned? No peakin' or tweakin'!](#) - Nick Vidal,Richard Zak

[CPV - \(17:30-17:59 PDT\) - \[T\]OTPs are not as secure as you might believe](#) - Santiago Kantorowicz

[DC - Let's Dance in the Cache - Destabilizing Hash Table on Microsoft IIS](#) - Orange Tsai

[DC - cont...\(16:30-17:15 PDT\) - A dead man's full-yet-responsible-disclosure system](#) - Yolan Romailleur

[DC - \(17:30-17:50 PDT\) - Deanonymization of TOR HTTP hidden services](#) - Ionut Cernica

[DC - cont...\(08:00-18:59 PDT\) - Human Registration Open](#)

[DC - Hunting Bugs in The Tropics](#) - Daniel Jensen

[DC - cont...\(16:30-17:15 PDT\) - DEF CON Policy Dept - Special Edition Policy Talk](#) - DEF CON Policy Dept

[DC - \(17:30-18:15 PDT\) - DEF CON Policy Dept - Special Edition Policy Talk](#) - DEF CON Policy Dept

[DC - cont...\(10:00-17:59 PDT\) - Vendor Area Open](#)

[DC - cont...\(10:00-17:59 PDT\) - Village Areas Open \(Generally\)](#) -

[HHV - cont...\(10:00-17:59 PDT\) - Solder Skills Village](#) - Open

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

[IOTV - cont...\(10:00-17:59 PDT\) - Hands on Hardware Hacking - eMMC to Root](#) - Deral Heiland

[IOTV - cont...\(10:00-17:59 PDT\) - Drone Hack](#) -

[IOTV - cont...\(10:00-17:59 PDT\) - IoT Village CTF](#) -

[IOTV - cont...\(10:00-17:59 PDT\) - IoT Village CTF Challenges](#) -

[IOTV - cont...\(10:00-17:59 PDT\) - Hands on hacking labs](#) -

[PLV - cont...\(16:00-17:45 PDT\) - Election Security Bridge Building](#) - Jack Cable,Trevor Timmons,Michael Ross

[PLV - cont...\(16:00-17:45 PDT\) - Moving Regulation Upstream - An Increasing focus on the Role of Digital Service Providers](#) - Jen Ellis,Irfan Hemani,Adam Dobell

[SKY - Deadly Russian Malware in Ukraine](#) - Chris Kubecka

[SOC - Meet the Digital Lab at Consumer Reports](#) -

[SOC - cont...\(09:00-17:59 PDT\) - Chillout Lounge - Entertainment](#) - Rusty,s1gns0f1fe,Pie & Darren,Merin MC,Kampf,djdead

[SOC - cont...\(16:00-17:59 PDT\) - Queercon Mixer](#) -

[SOC - EFF Tech Trivia](#) -

[SOC - cont...\(16:00-18:59 PDT\) - DC404/DC678/DC770/DC470 \(Atlanta Metro\) Meetup](#) -

[SOC - Friends of Bill W](#) -

[SOC - cont...\(16:00-18:59 PDT\) - DEF CON Holland DC3115 & DC3120 Group Meetup](#) -

[WS - cont...\(15:00-18:59 PDT\) - Hacking the Metal 2: Hardware and the Evolution of C Creatures](#) - Eigentourist

[WS - cont...\(15:00-18:59 PDT\) - Hand On Mainframe Buffer Overflows - RCE Edition](#) - Phil Young,Jake Labelle

WS - cont...(15:00-18:59 PDT) - Securing Industrial Control Systems from the core: PLC secure coding practices - Arnaud Soullie,Alexandrine Torrents  
WS - cont...(15:00-18:59 PDT) - FROM ZERO TO HERO IN A BLOCKCHAIN SECURITY - Roman Zaikin,Dikla Barda,Oded Vanunu  
WS - cont...(15:00-18:59 PDT) - Securing Smart Contracts - Irvin Lemus,Kaitlyn Handleman,Elizabeth Biddlecome,Sam Bowne

## Friday - 18:00 PDT

---

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

---

DC - Pulling Passwords out of Configuration Manager: Practical Attacks against Microsoft's Endpoint Management Software - Christopher Panayi  
DC - Tear Down this Zywall: Breaking Open Zyxel Encrypted Firmware - Jay Lagorio  
DC - cont...(08:00-18:59 PDT) - Human Registration Open  
DC - Killer Hertz - Chris Rock  
DC - cont...(17:30-18:15 PDT) - DEF CON Policy Dept - Special Edition Policy Talk - DEF CON Policy Dept  
DC - (18:30-18:50 PDT) - Dragon Tails: Supply-side Security and International Vulnerability Disclosure Law - Stewart Scott,Trey Herr  
SOC - (18:30-21:30 PDT) - Girls Hack Village Meetup -  
SOC - cont...(17:00-19:59 PDT) - Meet the Digital Lab at Consumer Reports -  
SOC - Black & White Ball - Entertainment - Magician Kody Hildebrand,Miss Jackalope,n0x08,Skittish & Bus,Biolux,Dual Core,Ictre Normal,Keith Meyers  
SOC - cont...(17:00-19:59 PDT) - EFF Tech Trivia -  
SOC - cont...(16:00-18:59 PDT) - DC404/DC678/DC770/DC470 (Atlanta Metro) Meetup -  
SOC - cont...(16:00-18:59 PDT) - DEF CON Holland DC3115 & DC3120 Group Meetup -  
SOC - Lawyers Meet -  
WS - cont...(15:00-18:59 PDT) - Hacking the Metal 2: Hardware and the Evolution of C Creatures - Eigentourist  
WS - cont...(15:00-18:59 PDT) - Hand On Mainframe Buffer Overflows - RCE Edition - Phil Young,Jake Labelle  
WS - cont...(15:00-18:59 PDT) - Securing Industrial Control Systems from the core: PLC secure coding practices - Arnaud Soullie,Alexandrine Torrents  
WS - cont...(15:00-18:59 PDT) - FROM ZERO TO HERO IN A BLOCKCHAIN SECURITY - Roman Zaikin,Dikla Barda,Oded Vanunu  
WS - cont...(15:00-18:59 PDT) - Securing Smart Contracts - Irvin Lemus,Kaitlyn Handleman,Elizabeth Biddlecome,Sam Bowne

## Friday - 19:00 PDT

---

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

---

PLV - Meet the Feds: CISA Edition (Lounge) - CISA Staff  
SOC - cont...(18:30-21:30 PDT) - Girls Hack Village Meetup -  
SOC - cont...(17:00-19:59 PDT) - Meet the Digital Lab at Consumer Reports -  
SOC - (19:30-01:59 PDT) - Hacker Karaoke -  
SOC - cont...(17:00-19:59 PDT) - EFF Tech Trivia -

## Friday - 20:00 PDT

---

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

---

PLV - Meet the Feds: DHS Edition (Lounge) - DHS Staff  
SOC - Movie Night Double Feature - Arrival & Real Genius -  
SOC - cont...(18:30-21:30 PDT) - Girls Hack Village Meetup -

SOC - Hacker Jeopardy -  
SOC - Pilots and Hackers Meetup -  
SOC - BlueTeam Village Party -

## Friday - 21:00 PDT

---

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

---

PLV - cont...(20:00-21:59 PDT) - Meet the Feds: DHS Edition (Lounge) - DHS Staff  
SOC - cont...(20:00-23:59 PDT) - Movie Night Double Feature - Arrival & Real Genius -  
SOC - cont...(18:30-21:30 PDT) - Girls Hack Village Meetup -  
SOC - cont...(20:00-21:59 PDT) - Hacker Jeopardy -  
SOC - cont...(20:00-21:59 PDT) - Pilots and Hackers Meetup -  
SOC - GOTHCON (#DCGOTHCON) -  
SOC - Hallway Monitor Party - Entertainment - DJ UNIT 77 [ 0077 : 0077 ],CaptHz,DJ Scythe,Magik Plan,Tense Future  
SOC - cont...(20:00-22:59 PDT) - BlueTeam Village Party -

## Friday - 22:00 PDT

---

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

---

SOC - cont...(20:00-23:59 PDT) - Movie Night Double Feature - Arrival & Real Genius -  
SOC - Queercon Party -  
SOC - cont...(20:00-22:59 PDT) - BlueTeam Village Party -

## Friday - 23:00 PDT

---

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

---

SOC - cont...(20:00-23:59 PDT) - Movie Night Double Feature - Arrival & Real Genius -

# Saturday

---

This Schedule is tentative and may be changed at any time. Check at an Info Booth for the latest.

---

## Saturday - 09:00 PDT

---

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

---

DC - Human Registration Open  
DC - Merch (formerly swag) Area Open -- README -  
SKY - (09:30-10:20 PDT) - Confessions of a CISO - Laura Whitt-Winyard  
SOC - Chillout Lounge - Entertainment - Rusty,s1gns0f1fe,Pie & Darren,Merin MC,Kampf,djdead

## Saturday - 10:00 PDT

---

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

---

AIV - A few useful things to know about AI Red Teams - Sudipto Rakshit

ASV - Hack the Airport with Intelligenesis -  
ASV - Hack the Airfield with DDS -  
ASV - Building Your Own Satellite Ground Station - Eric Escobar  
ASV - Satellite Eavesdropping with DDS -  
ASV - Red Balloon Failsat Challenges -  
ASV - Pen Test Partners A320 Simulator -  
ASV - Hack-A-Sat Digital Twin Workshop -  
ASV - Amazon Web Services Aerospace and Satellite Jam -  
ASV - Boeing ARINC 429 Airplane Challenge and CTF -  
ASV - (10:30-10:55 PDT) - Quantum Snake Oil? What Ailments Can It Cure? - Jose Pizarro  
BHV - NASA + Healthcare ... - Dr. Josef Schmid  
BHV - (10:30-10:59 PDT) - Faking Positive COVID Tests - Ken Gannon  
BICV - When The "IT" Hits The Fan, Stick To the Plan - Levone Campbell  
BTV - (10:30-11:30 PDT) - Obsidian Forensics: KillChain3 - Continued Adventures in Splunk and Security Onion - Omenscan,Wes Lambert,ExtremePaperClip  
BTV - (10:30-11:30 PDT) - Obsidian: IR - OODA! An hour in incident responder life - juju43  
BTV - (10:30-11:30 PDT) - Obsidian CTH: Sniffing Compromise: Hunting for Bloodhound - CerealKiller  
CLV - OAuth-some Security Tricks: Yet more OAuth abuse - Jenko Hwong  
CLV - (10:40-11:20 PDT) - Who Contains the "Serverless" Containers? - Daniel Prizmant  
CPV - (10:30-10:59 PDT) - Fun with Factoring Large Prime Numbers - p80n,r3c0d3  
DC - Scaling the Security Researcher to Eliminate OSS Vulnerabilities Once and For All - Jonathan Leitschuh  
DC - Literal Self-Pwning: Why Patients - and Their Advocates - Should Be Encouraged to Hack, Improve, and Mod Med Tech - Christian "quaddi" Dameff MD,Jeff "r3plicant" Tully MD,Cory Doctorow  
DC - cont...(09:00-18:59 PDT) - Human Registration Open  
DC - Brazil Redux: Short Circuiting Tech-Enabled Dystopia with The Right to Repair - Paul Roberts,Corynne McSherry,Joe Grand,Louis Rossmann,Kyle Wiens  
DC - Vendor Area Open  
DC - cont...(09:00-15:59 PDT) - Merch (formerly swag) Area Open -- README -  
DC - Village Areas Open (Generally) -  
DDV - DDV open and accepting drives for duplication -  
DL - Empire 4.0 and Beyond - Vincent "Vinnybod" Rose,Anthony "Cx01N" Rose  
DL - Memfini - A systemwide memory monitor interface for linux - Shubham Dubey,Rishal Dwivedi  
DL - svachal + machinescli - Ankur Tyagi  
DL - Injectyll-HIDe: Pushing the Future of Hardware Implants to the Next Level - Jonathan Fischer,Jeremy Miller  
DL - EDR detection mechanisms and bypass techniques with EDRSandBlast - Maxime Meignan,Thomas Diot  
HHV - Solder Skills Village - Open  
HHV - Hardware Hacking Village - Open  
IOTV - Hands on Hardware Hacking – eMMC to Root - Deral Heiland  
IOTV - Drone Hack -  
IOTV - IoT Village CTF -  
IOTV - BURP Suite, Forensics Tools & 0-day Exploit Development. - Ken Pyle  
IOTV - IoT Village CTF Challenges -  
IOTV - Hands on hacking labs -  
LPV - (10:15-10:45 PDT) - Intro to Lockpicking - TOOOL  
MIV - Tools for Fighting Disinformation - Preslav Nakov  
MIV - (10:45-12:30 PDT) - Mass Disinformation Operations - How to detect and assess Ops with OSINT & SOCMINT tools and techniques - Paula González Nagore  
PLV - Hacking Operational Collaboration - David Forscay  
PLV - Imagining a cyber policy crisis: Storytelling and Simulation for real-world risks - Winnona DeSombre,Safa Shahwan Edwards,Nina Kollars  
SKY - cont...(09:30-10:20 PDT) - Confessions of a CISO - Laura Whitt-Winyard  
SKY - (10:35-11:25 PDT) - What your stolen identity did on its CoViD vacation - Judge Taylor  
SOC - cont...(09:00-17:59 PDT) - Chillout Lounge - Entertainment - Rusty,s1gnsof1ife,Pie & Darren,Merin MC,Kampf,djdead  
WS - Pivoting, Tunneling, and Redirection Master Class - Barrett Darnell,Wesley Thurner

WS - Master Class: Delivering a New Construct in Advanced Volatile Memory Analysis for Fun and Profit - Solomon Sonya  
WS - Dig Dug: The Lost Art of Network Tunneling - Eijah,Cam  
WS - Windows Defence Evasion and Fortification Primitives - Rohan Durve,Paul Laîné  
WS - CTF 101: Breaking into CTFs (or “The Petting Zoo” - Breaking into CTFs) - Robert Fitzpatrick,Chris Forte

## Saturday - 11:00 PDT

---

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

---

AIV - Hands-on Hacking of Reinforcement Learning Systems - Dr. Amanda Minnich  
ASV - cont...(10:00-16:59 PDT) - Hack the Airport with Intelligenesis -  
ASV - cont...(10:00-16:59 PDT) - Hack the Airfield with DDS -  
ASV - cont...(10:00-16:59 PDT) - Satellite Eavesdropping with DDS -  
ASV - cont...(10:00-15:59 PDT) - Red Balloon Failsat Challenges -  
ASV - cont...(10:00-11:59 PDT) - Pen Test Partners A320 Simulator -  
ASV - cont...(10:00-16:59 PDT) - Hack-A-Sat Digital Twin Workshop -  
ASV - cont...(10:00-16:59 PDT) - Amazon Web Services Aerospace and Satellite Jam -  
ASV - cont...(10:00-15:59 PDT) - Boeing ARINC 429 Airplane Challenge and CTF -  
ASV - Cyber Threats Against Aviation Systems: The Only Threat Briefing You Really Need - Teresa Merklin  
BHV - How to Leverage MDS2 Data for Medical Device Security - Jeremy Linden  
BHV - (11:30-11:59 PDT) - All information should be free (except the brain data you want to keep in your head) - Isabel Straw  
BICV - Cryptocurrency: A Bridge Across the Digital Divide - Stephanie Barnes  
BTV - cont...(10:30-11:30 PDT) - Obsidian Forensics: KillChain3 - Continued Adventures in Splunk and Security Onion - Omenscan,Wes Lambert,ExtremePaperClip  
BTV - cont...(10:30-11:30 PDT) - Obsidian: IR - OODA! An hour in incident responder life - juju43  
BTV - (11:30-12:30 PDT) - Obsidian Forensics: Kill Chain 3 Endpoint Forensics Walkthrough - Omenscan  
BTV - cont...(10:30-11:30 PDT) - Obsidian CTH: Sniffing Compromise: Hunting for Bloodhound - CerealKiller  
BTV - (11:30-12:30 PDT) - Obsidian CTI: Operationalizing Threat Intelligence - Stephanie G.,l00sid,ttheveii0x  
BTV - Threat Hunt Trilogy: A Beast in the Shadow! - Dr. Meisam Eslahi  
BTV - Web Shell Hunting - Joe Schottman  
CLV - cont...(10:40-11:20 PDT) - Who Contains the “Serverless” Containers? - Daniel Prizmant  
CLV - (11:20-11:59 PDT) - Purple Teaming & Adversary Emulation in the Cloud with Stratus Red Team - Christophe Tafani-Dereeper  
CPV - Introducing the Abusability Testing Framework (V1) - Nicole Chi,Ji Su Yoo,Avi Zajac  
CPV - (11:30-12:30 PDT) - Jailed By a Google Search Part 2: Abortion Surveillance in Post-Roe America - Kate Bertash  
DC - No-Code Malware: Windows 11 At Your Service - Michael Bargury  
DC - How To Get MUMPS Thirty Years Later (or, Hacking The Government via FOIA'd Code) - Zachary Minneker  
DC - cont...(09:00-18:59 PDT) - Human Registration Open  
DC - cont...(10:00-11:15 PDT) - Brazil Redux: Short Circuiting Tech-Enabled Dystopia with The Right to Repair - Paul Roberts,Corynne McSherry,Joe Grand,Louis Rossmann,Kyle Wiens  
DC - (11:30-12:15 PDT) - Reversing the Original Xbox Live Protocols - Tristan Miller  
DC - My First Hack Was in 1958 (Then A Career in Rock'n'Roll Taught Me About Security) - Winn Schwartau  
DC - cont...(10:00-17:59 PDT) - Vendor Area Open  
DC - cont...(09:00-15:59 PDT) - Merch (formerly swag) Area Open -- README -  
DC - cont...(10:00-17:59 PDT) - Village Areas Open (Generally) -  
DDV - cont...(10:00-16:59 PDT) - DDV open and accepting drives for duplication -  
DL - cont...(10:00-11:55 PDT) - Empire 4.0 and Beyond - Vincent "Vinnybod" Rose,Anthony "Cx01N" Rose  
DL - cont...(10:00-11:55 PDT) - Memfini - A systemwide memory monitor interface for linux - Shubham Dubey,Rishal Dwivedi  
DL - cont...(10:00-11:55 PDT) - svachal + machinescli - Ankur Tyagi  
DL - cont...(10:00-11:55 PDT) - Injectyll-HIDE: Pushing the Future of Hardware Implants to the Next Level - Jonathan Fischer,Jeremy Miller  
DL - cont...(10:00-11:55 PDT) - EDR detection mechanisms and bypass techniques with EDRSandBlast - Maxime Meignan,Thomas Diot

HHV - cont...(10:00-17:59 PDT) - Solder Skills Village - Open  
HHV - cont...(10:00-17:59 PDT) - Hardware Hacking Village - Open  
HRV - Free Amateur Radio License Exams -  
HRV - (11:30-11:59 PDT) - Ham Nets 101 - Jon Marler  
IOTV - cont...(10:00-17:59 PDT) - Hands on Hardware Hacking – eMMC to Root - Deral Heiland  
IOTV - cont...(10:00-17:59 PDT) - Drone Hack -  
IOTV - cont...(10:00-17:59 PDT) - IoT Village CTF -  
IOTV - cont...(10:00-13:59 PDT) - BURP Suite, Forensics Tools & 0-day Exploit Development. - Ken Pyle  
IOTV - cont...(10:00-17:59 PDT) - IoT Village CTF Challenges -  
IOTV - cont...(10:00-17:59 PDT) - Hands on hacking labs -  
LPV - Metal and Fire... Copying Keys via Mold and Cast Tactics - Deviant Ollam  
MIV - cont...(10:45-12:30 PDT) - Mass Disinformation Operations - How to detect and assess Ops with OSINT & SOCMINT tools and techniques - Paula González Nagore  
PLV - cont...(10:00-11:45 PDT) - Hacking Operational Collaboration - David Forscley  
PLV - cont...(10:00-11:45 PDT) - Imagining a cyber policy crisis: Storytelling and Simulation for real-world risks - Winnona DeSombre,Safa Shahwan Edwards,Nina Kollars  
PWV - So long, PBKDF2! The end of password-based key derivation - Vivek Nair  
RHV - Ethical considerations in using digital footprints for verifying identities for online services - Larsbodian  
SKY - cont...(10:35-11:25 PDT) - What your stolen identity did on its CoViD vacation - Judge Taylor  
SKY - (11:40-12:30 PDT) - This one time, at this Hospital, I got Ransomware - Eirick Luraas  
SOC - cont...(09:00-17:59 PDT) - Chillout Lounge - Entertainment - Rusty,s1gnsof1fe,Pie & Darren,Merin  
MC,Kampf,djdead  
WS - cont...(10:00-13:59 PDT) - Pivoting, Tunneling, and Redirection Master Class - Barrett Darnell,Wesley Thurner  
WS - cont...(10:00-13:59 PDT) - Master Class: Delivering a New Construct in Advanced Volatile Memory Analysis for Fun and Profit - Solomon Sonya  
WS - cont...(10:00-13:59 PDT) - Dig Dug: The Lost Art of Network Tunneling - Ejiah,Cam  
WS - cont...(10:00-13:59 PDT) - Windows Defence Evasion and Fortification Primitives - Rohan Durve,Paul Laîné  
WS - cont...(10:00-13:59 PDT) - CTF 101: Breaking into CTFs (or “The Petting Zoo” - Breaking into CTFs) - Robert Fitzpatrick,Chris Forte

## Saturday - 12:00 PDT

---

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

---

AIV - A System for Alert Prioritization - Ben Gelman ,Salma Taoufiq  
ASV - cont...(10:00-16:59 PDT) - Hack the Airport with Intelligenesis -  
ASV - cont...(10:00-16:59 PDT) - Hack the Airfield with DDS -  
ASV - cont...(10:00-16:59 PDT) - Satellite Eavesdropping with DDS -  
ASV - cont...(10:00-15:59 PDT) - Red Balloon Failsat Challenges -  
ASV - cont...(10:00-16:59 PDT) - Hack-A-Sat Digital Twin Workshop -  
ASV - cont...(10:00-16:59 PDT) - Amazon Web Services Aerospace and Satellite Jam -  
ASV - cont...(10:00-15:59 PDT) - Boeing ARINC 429 Airplane Challenge and CTF -  
ASV - Hack-A-Sat Aerospace PiSat Challenge -  
ASV - Introduction to Aircraft Networks and Security Design Considerations - Sean Sullivan  
BHV - Breaking the Intelligence Cycle - how to tailor intelligence function to your needs? - Ohad Zaidenberg  
BICV - Decolonizing Cybersecurity - Birhanu Eshete  
BTV - cont...(11:30-12:30 PDT) - Obsidian Forensics: Kill Chain 3 Endpoint Forensics Walkthrough - Omenscan  
BTV - cont...(11:30-12:30 PDT) - Obsidian CTI: Operationalizing Threat Intelligence - Stephanie G.,l00sid,ttheveii0x  
BTV - (12:15-12:45 PDT) - Even my Dad is a Threat Modeler! - Sarthak Taneja  
BTV - cont...(11:00-14:59 PDT) - Web Shell Hunting - Joe Schottman  
CLV - SquarePhish - Phishing Office 365 using QR Codes and OAuth 2.0 Device Code Flow - Kamron Talebzadeh,Nevada  
Romsdahl  
CLV - (12:30-13:10 PDT) - Security Misconfigurations in the Cloud - "Oh Look, something fluffy, poke, poke, poke" - Kat Fitzgerald  
CPV - cont...(11:30-12:30 PDT) - Jailed By a Google Search Part 2: Abortion Surveillance in Post-Roe America - Kate

Bertash

DC - All Roads leads to GKE's Host : 4+ Ways to Escape - Billy Jheng,Muhammad ALifa Ramdhan  
DC - The Evil PLC Attack: Weaponizing PLCs - Sharon Brizinov  
DC - (12:30-13:15 PDT) - Analyzing PIPEDREAM: Challenges in testing an ICS attack toolkit. - Jimmy Wylie  
DC - cont...(09:00-18:59 PDT) - Human Registration Open  
DC - cont...(11:30-12:15 PDT) - Reversing the Original Xbox Live Protocols - Tristan Miller  
DC - (12:30-12:50 PDT) - The hitchhacker's guide to iPhone Lightning & JTAG hacking - stacksmashing  
DC - Tracking Military Ghost Helicopters over our Nation's Capital - Andrew Logan  
DC - (12:30-13:15 PDT) - UFOs, Alien Life, and the Least Untruthful Things I Can Say. - Richard Thieme  
DC - cont...(10:00-17:59 PDT) - Vendor Area Open  
DC - cont...(09:00-15:59 PDT) - Merch (formerly swag) Area Open -- README -  
DC - cont...(10:00-17:59 PDT) - Village Areas Open (Generally) -  
DDV - cont...(10:00-16:59 PDT) - DDV open and accepting drives for duplication -  
DL - alsanna - Jason Johnson  
DL - unblob - towards efficient firmware extraction - Quentin Kaiser,Florian Lukavsky  
DL - PMR - PT & VA Management & Reporting - Abdul Alanazi,Musaed Bin Muatred  
DL - Defensive 5G - Ryan Ashley,Eric Mair  
DL - SharpSCCM - Chris Thompson,Duane Michael  
HHV - cont...(10:00-17:59 PDT) - Solder Skills Village - Open  
HHV - cont...(10:00-17:59 PDT) - Hardware Hacking Village - Open  
HRV - cont...(11:00-16:59 PDT) - Free Amateur Radio License Exams -  
IOTV - cont...(10:00-17:59 PDT) - Hands on Hardware Hacking – eMMC to Root - Deral Heiland  
IOTV - cont...(10:00-17:59 PDT) - Drone Hack -  
IOTV - cont...(10:00-17:59 PDT) - IoT Village CTF -  
IOTV - cont...(10:00-13:59 PDT) - BURP Suite, Forensics Tools & 0-day Exploit Development. - Ken Pyle  
IOTV - cont...(10:00-17:59 PDT) - IoT Village CTF Challenges -  
IOTV - cont...(10:00-17:59 PDT) - Hands on hacking labs -  
LPV - Dozier Drill Tournament  
MIV - cont...(10:45-12:30 PDT) - Mass Disinformation Operations - How to detect and assess Ops with OSINT & SOCMINT tools and techniques - Paula González Nagore  
MIV - (12:30-13:45 PDT) - Cognitive Security in Theory and Practice - Sara-Jayne Terp  
PLV - Hacking Aviation Policy - Timothy Weston,Ayan Islam,Meg King,Ken Munro,Pete Cooper  
PLV - Addressing the gap in assessing (or measuring) the harm of cyberattacks - Adrien Ogee  
SKY - cont...(11:40-12:30 PDT) - This one time, at this Hospital, I got Ransomware - Eirick Luraas  
SKY - (12:45-13:35 PDT) - Voter Targeting, Location Data, and You - 10ngrange  
SOC - cont...(09:00-17:59 PDT) - Chillout Lounge - Entertainment - Rusty,s1gnsoflife,Pie & Darren,Merin  
MC,Kampf,djdead  
SOC - No Starch Press - Book Signing - Corey Ball, Hacking APIs  
SOC - Friends of Bill W -  
WS - cont...(10:00-13:59 PDT) - Pivoting, Tunneling, and Redirection Master Class - Barrett Darnell,Wesley Thurner  
WS - cont...(10:00-13:59 PDT) - Master Class: Delivering a New Construct in Advanced Volatile Memory Analysis for Fun and Profit - Solomon Sonya  
WS - cont...(10:00-13:59 PDT) - Dig Dug: The Lost Art of Network Tunneling - Ejiah,Cam  
WS - cont...(10:00-13:59 PDT) - Windows Defence Evasion and Fortification Primitives - Rohan Durve,Paul Laîné  
WS - cont...(10:00-13:59 PDT) - CTF 101: Breaking into CTFs (or “The Petting Zoo” - Breaking into CTFs) - Robert Fitzpatrick,Chris Forte

## Saturday - 13:00 PDT

---

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

---

AIV - CatPhish Automation - The Emerging Use of Artificial Intelligence in Social Engineering - Justin Hutchens  
ASV - cont...(10:00-16:59 PDT) - Hack the Airport with Intelligenesis -  
ASV - cont...(10:00-16:59 PDT) - Hack the Airfield with DDS -  
ASV - cont...(10:00-16:59 PDT) - Satellite Eavesdropping with DDS -

ASV - cont...(10:00-15:59 PDT) - Red Balloon Failsat Challenges -  
ASV - cont...(10:00-16:59 PDT) - Hack-A-Sat Digital Twin Workshop -  
ASV - cont...(10:00-16:59 PDT) - Amazon Web Services Aerospace and Satellite Jam -  
ASV - cont...(10:00-15:59 PDT) - Boeing ARINC 429 Airplane Challenge and CTF -  
ASV - cont...(12:00-16:59 PDT) - Hack-A-Sat Aerospace PiSat Challenge -  
ASV - Resumé Review and Career Guidance Session -  
ASV - Pen Test Partners A320 Simulator -  
ASV - Hunting for Spacecraft Zero Days Using Digital Twins - Brandon Bailey  
BHV - Out of the Abyss: Surviving Vulnerability Management - Leo Nendza,Mike Kijewski  
BHV - (13:30-14:30 PDT) - Radical inclusivity and intersectionality in the biohacking world - Berkelly Gonzalez  
BICV - State of the Model - Jovonni Pharr,GACWR Team  
BTV - Obsidian CTH Live: Killchain 3 Walkthrough -  
BTV - Obsidian: IR - Final Reporting Made Exciting\* - aviditas,CountZ3r0  
BTV - Obsidian REM: Phishing In The Morning: An Abundance of Samples! - Alison N  
BTV - The DFIR Report Homecoming Parade Panel - Kostas,ICSNick - Nicklas Keijser,Ch33r10,Justin Elze,Jamie Williams,nas\_bench - Nasreddine Bencherchali  
BTV - cont...(11:00-14:59 PDT) - Web Shell Hunting - Joe Schottman  
CLV - cont...(12:30-13:10 PDT) - Security Misconfigurations in the Cloud - "Oh Look, something fluffy, poke, poke, poke" - Kat Fitzgerald  
CLV - BrokenbyDesign: Azure | Get started with hacking Azure - Siebren Kraak,Roy Stultiens,Ricardo Sanchez,Ricardo Sanchez  
CLV - (13:40-14:20 PDT) - us-east-1 Shuffle: Lateral Movement and other Creative Steps Attackers Take in AWS Cloud Environments and how to detect them - Felipe Espósito  
CPV - Cryptle: a secure multi-party Wordle clone with Enarx - Tom Dohrmann,Richard Zak,Nick Vidal  
CPV - (13:45-14:30 PDT) - Exploring Unprecedented Avenues for Data Harvesting in the Metaverse - Gonzalo Munilla Garrido,Vivek Nair  
DC - Exploring Ancient Ruins to Find Modern Bugs: Discovering a 0-Day in an MS-RPC Service - Ophir Harpaz,Ben Barnea  
DC - cont...(12:30-13:15 PDT) - Analyzing PIPEDREAM: Challenges in testing an ICS attack toolkit. - Jimmy Wylie  
DC - (13:30-14:15 PDT) - Do Not Trust the ASA, Trojans! - Jacob Baines  
DC - cont...(09:00-18:59 PDT) - Human Registration Open  
DC - Chromebook Breakout: Escaping Jail, with your friends, using a Pico Ducky - Jimi Allee  
DC - cont...(12:30-13:15 PDT) - UFOs, Alien Life, and the Least Untruthful Things I Can Say. - Richard Thieme  
DC - (13:30-14:15 PDT) - HACK THE HEMISPHERE! How we (legally) broadcasted hacker content to all of North America using an end-of-life geostationary satellite, and how you can set up your own broadcast too! - Andrew Green,Karl Koscher  
DC - cont...(10:00-17:59 PDT) - Vendor Area Open  
DC - cont...(09:00-15:59 PDT) - Merch (formerly swag) Area Open -- README -  
DC - cont...(10:00-17:59 PDT) - Village Areas Open (Generally) -  
DDV - cont...(10:00-16:59 PDT) - DDV open and accepting drives for duplication -  
DL - cont...(12:00-13:55 PDT) - alsanna - Jason Johnson  
DL - cont...(12:00-13:55 PDT) - unblob - towards efficient firmware extraction - Quentin Kaiser,Florian Lukavsky  
DL - cont...(12:00-13:55 PDT) - PMR - PT & VA Management & Reporting - Abdul Alanazi,Musaed Bin Muatred  
DL - cont...(12:00-13:55 PDT) - Defensive 5G - Ryan Ashley,Eric Mair  
DL - cont...(12:00-13:55 PDT) - SharpSCCM - Chris Thompson,Duane Michael  
HHV - cont...(10:00-17:59 PDT) - Solder Skills Village - Open  
HHV - cont...(10:00-17:59 PDT) - Hardware Hacking Village - Open  
HHV - RoboSumo -  
HRV - cont...(11:00-16:59 PDT) - Free Amateur Radio License Exams -  
HRV - Getting on the air: My experiences with Ham radio QRP - Jeremy Hong  
IOTV - cont...(10:00-17:59 PDT) - Hands on Hardware Hacking – eMMC to Root - Deral Heiland  
IOTV - cont...(10:00-17:59 PDT) - Drone Hack -  
IOTV - cont...(10:00-17:59 PDT) - IoT Village CTF -  
IOTV - cont...(10:00-13:59 PDT) - BURP Suite, Forensics Tools & 0-day Exploit Development. - Ken Pyle  
IOTV - cont...(10:00-17:59 PDT) - IoT Village CTF Challenges -  
IOTV - cont...(10:00-17:59 PDT) - Hands on hacking labs -  
LPV - cont...(12:00-13:59 PDT) - Dozier Drill Tournament

LPV - Intro to Lockpicking - TOOOL

MIV - cont...(12:30-13:45 PDT) - Cognitive Security in Theory and Practice - Sara-Jayne Terp

PLV - cont...(12:00-13:45 PDT) - Hacking Aviation Policy - Timothy Weston,Ayan Islam,Meg King,Ken Munro,Pete Cooper

PLV - cont...(12:00-13:45 PDT) - Addressing the gap in assessing (or measuring) the harm of cyberattacks - Adrien Ogee

SKY - cont...(12:45-13:35 PDT) - Voter Targeting, Location Data, and You - 10ngrange

SKY - (13:50-15:40 PDT) - INTERNET WARS 2022: These wars aren't just virtual - Jivesx,Russ Handorf,Chris

Kubecka,Harri Hursti,Cheryl Biswall,Bryson Bort,Gadi Evron

SOC - cont...(09:00-17:59 PDT) - Chillout Lounge - Entertainment - Rusty,s1gnsof1fe,Pie & Darren,Merin MC,Kampf,djdead

SOC - No Starch Press - Book Signing - Joe Gray, Practical Social Engineering

WS - cont...(10:00-13:59 PDT) - Pivoting, Tunneling, and Redirection Master Class - Barrett Darnell,Wesley Thurner

WS - cont...(10:00-13:59 PDT) - Master Class: Delivering a New Construct in Advanced Volatile Memory Analysis for Fun and Profit - Solomon Sonya

WS - cont...(10:00-13:59 PDT) - Dig Dug: The Lost Art of Network Tunneling - Eijah,Cam

WS - cont...(10:00-13:59 PDT) - Windows Defence Evasion and Fortification Primitives - Rohan Durve,Paul Laîné

WS - cont...(10:00-13:59 PDT) - CTF 101: Breaking into CTFs (or “The Petting Zoo” - Breaking into CTFs) - Robert Fitzpatrick,Chris Forte

## Saturday - 14:00 PDT

---

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

---

AIV - The Use of AI/ML in Offensive Security Operations -

ASV - cont...(10:00-16:59 PDT) - Hack the Airport with Intelligenesis -

ASV - cont...(10:00-16:59 PDT) - Hack the Airfield with DDS -

ASV - cont...(10:00-16:59 PDT) - Satellite Eavesdropping with DDS -

ASV - cont...(10:00-15:59 PDT) - Red Balloon Failsat Challenges -

ASV - cont...(10:00-16:59 PDT) - Hack-A-Sat Digital Twin Workshop -

ASV - cont...(10:00-16:59 PDT) - Amazon Web Services Aerospace and Satellite Jam -

ASV - cont...(10:00-15:59 PDT) - Boeing ARINC 429 Airplane Challenge and CTF -

ASV - cont...(12:00-16:59 PDT) - Hack-A-Sat Aerospace PiSat Challenge -

ASV - cont...(13:00-14:59 PDT) - Resumé Review and Career Guidance Session -

ASV - cont...(13:00-14:59 PDT) - Pen Test Partners A320 Simulator -

ASV - Vulnerability Assessment of a Satellite Simulator - Henry Haswell

ASV - (14:30-14:55 PDT) - The Emerging Space - Cyber Warfare Theatre - Eytan Tepper

BHV - cont...(13:30-14:30 PDT) - Radical inclusivity and intersectionality in the biohacking world - Berkelly Gonzalez

BHV - (14:30-14:59 PDT) - Natural Disasters and International Supply Chains: Biomedical and Pharmaceutical Review - Jorge Acevedo Canabal

BTV - Obsidian Live: May We Have the OODA Loops? - CountZ3r0,juju43

BTV - Obsidian Forensics: Using Chainsaw to Identify Malicious Activity - Danny D. Henderson Jr (B4nd1t0)

BTV - (14:30-14:59 PDT) - Obsidian Forensics: Creating a custom Velociraptor collector - Wes Lambert,Omenscan

BTV - Obsidian CTH: The Logs are Gone? - ExtremePaperClip

BTV - (14:15-14:45 PDT) - Hunting Malicious Office Macros - Anton Ovrutsky

BTV - cont...(11:00-14:59 PDT) - Web Shell Hunting - Joe Schottman

CLV - cont...(13:40-14:20 PDT) - us-east-1 Shuffle: Lateral Movement and other Creative Steps Attackers Take in AWS

Cloud Environments and how to detect them - Felipe Espósito

CLV - (14:20-14:50 PDT) - Access Undenied on AWS - Troubleshooting AWS IAM AccessDenied Errors - Noam Dahan

CPV - cont...(13:45-14:30 PDT) - Exploring Unprecedented Avenues for Data Harvesting in the Metaverse - Gonzalo Munilla Garrido,Vivek Nair

CPV - (14:30-14:59 PDT) - The deadly state of surveillance capitalism in healthcare - Valencia Robinson,Mike Mittelman,Andrea Downing

DC - The COW (Container On Windows) Who Escaped the Silo - Eran Segal

DC - cont...(13:30-14:15 PDT) - Do Not Trust the ASA, Trojans! - Jacob Baines

DC - (14:30-15:15 PDT) - Doing the Impossible: How I Found Mainframe Buffer Overflows - Jake Labelle

DC - cont...(09:00-18:59 PDT) - Human Registration Open

DC - OpenCola. The AntiSocial Network - John Midgley  
DC - cont...(13:30-14:15 PDT) - HACK THE HEMISPHERE! How we (legally) broadcasted hacker content to all of North America using an end-of-life geostationary satellite, and how you can set up your own broadcast too! - Andrew Green,Karl Koscher  
DC - (14:30-14:50 PDT) - Digging into Xiaomi's TEE to get to Chinese money - Slava Makkaveev  
DC - cont...(10:00-17:59 PDT) - Vendor Area Open  
DC - cont...(09:00-15:59 PDT) - Merch (formerly swag) Area Open -- README -  
DC - cont...(10:00-17:59 PDT) - Village Areas Open (Generally) -  
DDV - cont...(10:00-16:59 PDT) - DDV open and accepting drives for duplication -  
DL - OpenTDF - Paul Flynn,Cassandra Bailey  
DL - Control Validation Compass – Threat Modeling Aide & Purple Team Content Repo - Scott Small  
DL - ResidueFree - Logan Arkema  
DL - hls4ml - Open Source Machine Learning Accelerators on FPGAs - Ben Hawks,Andres Meza  
DL - Xavier Memory Analysis Framework - Solomon Sonya  
HHV - cont...(10:00-17:59 PDT) - Solder Skills Village - Open  
HHV - cont...(10:00-17:59 PDT) - Hardware Hacking Village - Open  
HRV - cont...(11:00-16:59 PDT) - Free Amateur Radio License Exams -  
IOTV - cont...(10:00-17:59 PDT) - Hands on Hardware Hacking – eMMC to Root - Deral Heiland  
IOTV - cont...(10:00-17:59 PDT) - Drone Hack -  
IOTV - cont...(10:00-17:59 PDT) - IoT Village CTF -  
IOTV - cont...(10:00-17:59 PDT) - IoT Village CTF Challenges -  
IOTV - cont...(10:00-17:59 PDT) - Hands on hacking labs -  
LPV - Please deposit 30c: A history of payphone locks that lead to one of the most secure locks ever made. - N thing  
MIV - (14:15-14:45 PDT) - 404! Memory Holing and the SEO Warping of Human History - Arikia Millikan  
MIV - (14:45-15:15 PDT) - Web Monetization: A privacy-preserving and open way to earn from Content - Uchi Uchibeke  
PLV - Confronting Reality in Cyberspace: Foreign Policy for a Fragmented Internet - Neal Pollard,Jason Healey  
PLV - Return-Oriented Policy Making for Open Source and Software Security - Trey Herr,Eric Mill,Harry Mourtos,Jack Cable  
SKY - cont...(13:50-15:40 PDT) - INTERNET WARS 2022: These wars aren't just virtual - Jivesx,Russ Handorf,Chris Kubecka,Harri Hursti,Cheryl Biswall,Bryson Bort,Gadi Evron  
SOC - cont...(09:00-17:59 PDT) - Chillout Lounge - Entertainment - Rusty,s1gnsoflife,Pie & Darren,Merin MC,Kampf,djdead  
SOC - No Starch Press - Book Signing - Jon DiMaggio, The Art of Cyberwarfare

## Saturday - 15:00 PDT

---

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

---

AIV - Generative Art Tutorial -  
ASV - cont...(10:00-16:59 PDT) - Hack the Airport with Intelligenesis -  
ASV - cont...(10:00-16:59 PDT) - Hack the Airfield with DDS -  
ASV - cont...(10:00-16:59 PDT) - Satellite Eavesdropping with DDS -  
ASV - cont...(10:00-15:59 PDT) - Red Balloon Failsat Challenges -  
ASV - cont...(10:00-16:59 PDT) - Hack-A-Sat Digital Twin Workshop -  
ASV - cont...(10:00-16:59 PDT) - Amazon Web Services Aerospace and Satellite Jam -  
ASV - cont...(10:00-15:59 PDT) - Boeing ARINC 429 Airplane Challenge and CTF -  
ASV - cont...(12:00-16:59 PDT) - Hack-A-Sat Aerospace PiSat Challenge -  
ASV - Near and Far: Securing On and Off Planet Networks at JPL - Wes Gavins  
BHV - Secure by Design - Facilities design cybersecurity - David Brearley  
BICV - Threat hunting? Ain't nobody got time for that... - Nick Goborn  
BTV - Challenges in Control Validation - AJ King,Jake Williams,Kristen Cotten  
BTV - Horusec - Brazilian SAST help World - Gilmar Esteves  
CLV - KQL Kung Fu: Finding the Needle in the Haystack in Your Azure Environments - Darwin Salazar  
CPV - (15:30-16:15 PDT) - Capturing Chaos: Harvesting Environmental Entropy - Carey Parker  
DC - You Have One New Appwntment - Hacking Proprietary iCalendar Properties - Eugene Lim

DC - cont...(14:30-15:15 PDT) - Doing the Impossible: How I Found Mainframe Buffer Overflows - Jake Labelle  
DC - (15:30-16:15 PDT) - Perimeter Breached! Hacking an Access Control System - Sam Quinn,Steve Povolny  
DC - cont...(09:00-18:59 PDT) - Human Registration Open  
DC - Déjà Vu: Uncovering Stolen Algorithms in Commercial Products - Patrick Wardle,Tom McGuire  
DC - (15:30-15:50 PDT) - Automotive Ethernet Fuzzing: From purchasing ECU to SOME/IP fuzzing - Woongjo Choi,Soohwan Oh,Jonghyuk Song  
DC - The Big Rick: How I Rickrolled My High School District and Got Away With It - Minh Duong  
DC - (15:30-16:15 PDT) - Tor: Darknet Opsec By a Veteran Darknet Vendor & the Hackers Mentality - Sam Bent  
DC - cont...(10:00-17:59 PDT) - Vendor Area Open  
DC - cont...(09:00-15:59 PDT) - Merch (formerly swag) Area Open -- README -  
DC - cont...(10:00-17:59 PDT) - Village Areas Open (Generally) -  
DDV - cont...(10:00-16:59 PDT) - DDV open and accepting drives for duplication -  
DL - cont...(14:00-15:55 PDT) - OpenTDF - Paul Flynn,Cassandra Bailey  
DL - cont...(14:00-15:55 PDT) - Control Validation Compass – Threat Modeling Aide & Purple Team Content Repo - Scott Small  
DL - cont...(14:00-15:55 PDT) - ResidueFree - Logan Arkema  
DL - cont...(14:00-15:55 PDT) - hls4ml - Open Source Machine Learning Accelerators on FPGAs - Ben Hawks,Andres Meza  
DL - cont...(14:00-15:55 PDT) - Xavier Memory Analysis Framework - Solomon Sonya  
HHV - cont...(10:00-17:59 PDT) - Solder Skills Village - Open  
HHV - cont...(10:00-17:59 PDT) - Hardware Hacking Village - Open  
HRV - cont...(11:00-16:59 PDT) - Free Amateur Radio License Exams -  
HRV - Panel: Ask-a-ham -  
IOTV - cont...(10:00-17:59 PDT) - Hands on Hardware Hacking – eMMC to Root - Deral Heiland  
IOTV - cont...(10:00-17:59 PDT) - Drone Hack -  
IOTV - cont...(10:00-17:59 PDT) - IoT Village CTF -  
IOTV - cont...(10:00-17:59 PDT) - IoT Village CTF Challenges -  
IOTV - cont...(10:00-17:59 PDT) - Hands on hacking labs -  
MIV - cont...(14:45-15:15 PDT) - Web Monetization: A privacy-preserving and open way to earn from Content - Uchi Uchibeke  
MIV - (15:15-15:45 PDT) - Fireside Chat - Arikia Millikan,Uchi Uchibeke  
MIV - (15:45-16:15 PDT) - Ad it up: To minimize mis- and dis-information, we must reshape the ad tech business, not regulate speech - Jessica Dheere  
PLV - cont...(14:00-15:45 PDT) - Confronting Reality in Cyberspace: Foreign Policy for a Fragmented Internet - Neal Pollard,Jason Healey  
PLV - cont...(14:00-15:45 PDT) - Return-Oriented Policy Making for Open Source and Software Security - Trey Herr,Eric Mill,Harry Mourtos,Jack Cable  
SKY - cont...(13:50-15:40 PDT) - INTERNET WARS 2022: These wars aren't just virtual - Jivesx,Russ Handorf,Chris Kubecka,Harri Hursti,Cheryl Biswall,Bryson Bort,Gadi Evron  
SOC - cont...(09:00-17:59 PDT) - Chillout Lounge - Entertainment - Rusty,s1gnsoflife,Pie & Darren,Merin MC,Kampf,djdead  
WS - Hybrid Phishing Payloads: From Threat-actors to You - Magnus Stubman,Jon Christiansen  
WS - Creating and uncovering malicious containers. - Adrian Wood,Griffin Francis,David Mitchell  
WS - Evading Detection: A Beginner's Guide to Obfuscation - Anthony "Cx01N" Rose,Vincent "Vinnybod" Rose,Jake "Hubbl3" Krasnov  
WS - Securing Web Apps - Elizabeth Biddlecome,Kaitlyn Handleman,Irvin Lemus,Sam Bowne  
WS - Automated Debugging Under The Hood - Building A Programmable Windows Debugger From Scratch (In Python) - Sergei Frankoff,Sean Wilson

## Saturday - 16:00 PDT

---

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

---

AIV - AI Music Tutorial and Show - dadabots  
ASV - cont...(10:00-16:59 PDT) - Hack the Airport with Intelligenesis -  
ASV - cont...(10:00-16:59 PDT) - Hack the Airfield with DDS -

ASV - cont...(10:00-16:59 PDT) - Satellite Eavesdropping with DDS -  
ASV - cont...(10:00-16:59 PDT) - Hack-A-Sat Digital Twin Workshop -  
ASV - cont...(10:00-16:59 PDT) - Amazon Web Services Aerospace and Satellite Jam -  
ASV - cont...(12:00-16:59 PDT) - Hack-A-Sat Aerospace PiSat Challenge -  
ASV - Space ISAC: Protecting Our Space Assets -  
BHV - Call for Evidence: Informing the Biological Security Strategy - Mariam Elgabry  
BHV - (16:30-17:59 PDT) - How to Build DIY Lifesaving Medical Devices - Four Thieves Vinegar Collective  
BICV - Neurodiversity in Cybersecurity: Find Your Competitive Advantage! - Kassandra Pierre,Nathan Chung  
BTV - Making Your SOC Suck Less - Shawn Thomas,Carson Zimmerman,Sebastian Stein,Alissa Torres,Jackie Bow  
CLV - cont...(15:00-16:59 PDT) - KQL Kung Fu: Finding the Needle in the Haystack in Your Azure Environments - Darwin Salazar  
CPV - cont...(15:30-16:15 PDT) - Capturing Chaos: Harvesting Environmental Entropy - Carey Parker  
CPV - (16:15-16:59 PDT) - Toto, I've a feeling we're not on a VPN anymore - Jonathan Tomek  
DC - Low Code High Risk: Enterprise Domination via Low Code Abuse - Michael Bargury  
DC - cont...(15:30-16:15 PDT) - Perimeter Breached! Hacking an Access Control System - Sam Quinn,Steve Povolny  
DC - (16:30-17:15 PDT) - Defeating Moving Elements in High Security Keys - Bill Graydon  
DC - cont...(09:00-18:59 PDT) - Human Registration Open  
DC - Trailer Shouting: Talking PLC4TRUCKS Remotely with an SDR - Ben Gardiner,Chris Poore  
DC - cont...(15:30-16:15 PDT) - Tor: Darknet Opsec By a Veteran Darknet Vendor & the Hackers Mentality - Sam Bent  
DC - (16:30-17:15 PDT) - Why did you lose the last PS5 restock to a bot Top-performing app-hackers business modules, architecture, and techniques - Arik  
DC - cont...(10:00-17:59 PDT) - Vendor Area Open  
DC - cont...(10:00-17:59 PDT) - Village Areas Open (Generally) -  
DDV - cont...(10:00-16:59 PDT) - DDV open and accepting drives for duplication -  
HHV - cont...(10:00-17:59 PDT) - Solder Skills Village - Open  
HHV - cont...(10:00-17:59 PDT) - Hardware Hacking Village - Open  
HHV - Prizes announced for HHV Rube Goldberg Machine, Make Your Own Use Contest, and Bring the Other Half -  
HRV - cont...(11:00-16:59 PDT) - Free Amateur Radio License Exams -  
IOTV - cont...(10:00-17:59 PDT) - Hands on Hardware Hacking – eMMC to Root - Deral Heiland  
IOTV - cont...(10:00-17:59 PDT) - Drone Hack -  
IOTV - cont...(10:00-17:59 PDT) - IoT Village CTF -  
IOTV - cont...(10:00-17:59 PDT) - IoT Village CTF Challenges -  
IOTV - cont...(10:00-17:59 PDT) - Hands on hacking labs -  
LPV - Intro to Lockpicking - TOOOL  
MIV - cont...(15:45-16:15 PDT) - Ad it up: To minimize mis- and dis-information, we must reshape the ad tech business, not regulate speech - Jessica Dheere  
MIV - (16:15-16:45 PDT) - Not Feeling Yourself: User Spoofing and Other Disinformation Exploits - Erica Burgess  
PLV - International Government Action Against Ransomware - Adam Dobell,Irfan Hemani,Jen Ellis  
SKY - Dancing Around DRM - Game Tech Chris,  
SOC - cont...(09:00-17:59 PDT) - Chillout Lounge - Entertainment - Rusty,s1gnsoflife,Pie & Darren,Merin  
MC,Kampf,djdead  
SOC - Queercon Mixer -  
WS - cont...(15:00-18:59 PDT) - Hybrid Phishing Payloads: From Threat-actors to You - Magnus Stubman,Jon Christiansen  
WS - cont...(15:00-18:59 PDT) - Creating and uncovering malicious containers. - Adrian Wood,Griffin Francis,David Mitchell  
WS - cont...(15:00-18:59 PDT) - Evading Detection: A Beginner's Guide to Obfuscation - Anthony "Cx01N" Rose,Vincent "Vinnybod" Rose,Jake "Hubbl3" Krasnov  
WS - cont...(15:00-18:59 PDT) - Securing Web Apps - Elizabeth Biddlecome,Kaitlyn Handleman,Irvin Lemus,Sam Bowne  
WS - cont...(15:00-18:59 PDT) - Automated Debugging Under The Hood - Building A Programmable Windows Debugger From Scratch (In Python) - Sergei Frankoff,Sean Wilson

## Saturday - 17:00 PDT

---

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

---

AIV - cont...(16:00-17:30 PDT) - AI Music Tutorial and Show - dadabots  
BHV - cont...(16:30-17:59 PDT) - How to Build DIY Lifesaving Medical Devices - Four Thieves Vinegar Collective  
BTW - Latest and Greatest in Incident Response - Lauren Proehl,plug,LitMoose,Jess,zr0  
CPV - Pursuing Phone Privacy Protection [WORKSHOP] - Mauricio Tavares,Matt Nash  
DC - Internal Server Error: Exploiting Inter-Process Communication with new desynchronization primitives - Martin Doyhenard  
DC - cont...(16:30-17:15 PDT) - Defeating Moving Elements in High Security Keys - Bill Graydon  
DC - (17:30-18:15 PDT) - Black-Box Assessment of Smart Cards - Daniel Crowley  
DC - cont...(09:00-18:59 PDT) - Human Registration Open  
DC - Hacking The Farm: Breaking Badly Into Agricultural Devices. - Sick Codes  
DC - cont...(16:30-17:15 PDT) - Why did you lose the last PS5 restock to a bot Top-performing app-hackers business modules, architecture, and techniques - Arik  
DC - (17:30-18:15 PDT) - Crossing the KASM -- a webapp pentest story - Justin Gardner,Samuel Erb  
DC - cont...(10:00-17:59 PDT) - Vendor Area Open  
DC - cont...(10:00-17:59 PDT) - Village Areas Open (Generally) -  
HHV - cont...(10:00-17:59 PDT) - Solder Skills Village - Open  
HHV - cont...(10:00-17:59 PDT) - Hardware Hacking Village - Open  
IOTV - cont...(10:00-17:59 PDT) - Hands on Hardware Hacking – eMMC to Root - Deral Heiland  
IOTV - cont...(10:00-17:59 PDT) - Drone Hack -  
IOTV - cont...(10:00-17:59 PDT) - IoT Village CTF -  
IOTV - cont...(10:00-17:59 PDT) - IoT Village CTF Challenges -  
IOTV - cont...(10:00-17:59 PDT) - Hands on hacking labs -  
PLV - cont...(16:00-17:45 PDT) - International Government Action Against Ransomware - Adam Dobell,Irfan Hemani,Jen Ellis  
SKY - Coming Home to Def Con: A Deep Dive into the Real Essence and Ethos of Hacking - Richard Thieme  
SOC - cont...(09:00-17:59 PDT) - Chillout Lounge - Entertainment - Rusty,s1gnsoflife,Pie & Darren,Merin MC,Kampf,djdead  
SOC - cont...(16:00-17:59 PDT) - Queercon Mixer -  
SOC - Denial, Deception, and Drinks with Mitre Engage -  
SOC - Friends of Bill W -  
WS - cont...(15:00-18:59 PDT) - Hybrid Phishing Payloads: From Threat-actors to You - Magnus Stubman,Jon Christiansen  
WS - cont...(15:00-18:59 PDT) - Creating and uncovering malicious containers. - Adrian Wood,Griffin Francis,David Mitchell  
WS - cont...(15:00-18:59 PDT) - Evading Detection: A Beginner's Guide to Obfuscation - Anthony "Cx01N" Rose,Vincent "Vinnybod" Rose,Jake "Hubbl3" Krasnov  
WS - cont...(15:00-18:59 PDT) - Securing Web Apps - Elizabeth Biddlecome,Kaitlyn Handleman,Irvin Lemus,Sam Bowne  
WS - cont...(15:00-18:59 PDT) - Automated Debugging Under The Hood - Building A Programmable Windows Debugger From Scratch (In Python) - Sergei Frankoff,Sean Wilson

## Saturday - 18:00 PDT

---

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

---

DC - The CSRF Resurrections! Starring the Unholy Trinity: Service Worker of PWA, SameSite of HTTP Cookie, and Fetch - Dongsung Kim  
DC - cont...(17:30-18:15 PDT) - Black-Box Assessment of Smart Cards - Daniel Crowley  
DC - (18:30-18:50 PDT) - Digital Skeleton Keys - We've got a bone to pick with offline Access Control Systems - Miana E Windall,Micsen  
DC - cont...(09:00-18:59 PDT) - Human Registration Open  
DC - cont...(17:30-18:15 PDT) - Crossing the KASM -- a webapp pentest story - Justin Gardner,Samuel Erb  
SOC - Night of the Ninjas - Entertainment - Scotch and Bubbles,TAIKOPROJECT,Z3NPI,Zebbler Encanti Experience,CTRL/rsm,Krisz Klink,Magician Kody Hildebrand,Mass Accelerator  
SOC - cont...(17:00-18:59 PDT) - Denial, Deception, and Drinks with Mitre Engage -  
WS - cont...(15:00-18:59 PDT) - Hybrid Phishing Payloads: From Threat-actors to You - Magnus Stubman,Jon Christiansen  
WS - cont...(15:00-18:59 PDT) - Creating and uncovering malicious containers. - Adrian Wood,Griffin Francis,David

Mitchell

[WS](#) - cont...(15:00-18:59 PDT) - [Evading Detection: A Beginner's Guide to Obfuscation](#) - Anthony "Cx01N" Rose,Vincent "Vinnybod" Rose,Jake "Hubbl3" Krasnov

[WS](#) - cont...(15:00-18:59 PDT) - [Securing Web Apps](#) - Elizabeth Biddlecome,Kaitlyn Handleman,Irvin Lemus,Sam Bowne

[WS](#) - cont...(15:00-18:59 PDT) - [Automated Debugging Under The Hood - Building A Programmable Windows Debugger From Scratch \(In Python\)](#) - Sergei Frankoff,Sean Wilson

## Saturday - 19:00 PDT

---

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

---

[PLV](#) - [Do No Harm \(Lounge\)](#) - Seeyew Mo,Jessica Wilkerson,Jeff "r3plicant" Tully MD,Christian "quaddi" Dameff MD,Alissa Knight

[SOC](#) - (19:30-00:59 PDT) - [BlanketFort Con](#) -

[SOC](#) - (19:30-01:59 PDT) - [Hacker Karaoke](#) -

## Saturday - 20:00 PDT

---

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

---

[PLV](#) - cont...(19:00-21:59 PDT) - [Do No Harm \(Lounge\)](#) - Seeyew Mo,Jessica Wilkerson,Jeff "r3plicant" Tully MD,Christian "quaddi" Dameff MD,Alissa Knight

[SOC](#) - [Movie Night Double Feature - The Conversation & The 13th Floor](#) -

[SOC](#) - (20:30-23:59 PDT) - [Girls Hack Village 90's House Party](#) -

[SOC](#) - [Meet the EFF](#) -

[SOC](#) - [Hacker Flairgrounds](#) -

[SOC](#) - [Hacker Jeopardy](#) -

## Saturday - 21:00 PDT

---

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

---

[PLV](#) - cont...(19:00-21:59 PDT) - [Do No Harm \(Lounge\)](#) - Seeyew Mo,Jessica Wilkerson,Jeff "r3plicant" Tully MD,Christian "quaddi" Dameff MD,Alissa Knight

[SOC](#) - cont...(20:00-23:59 PDT) - [Movie Night Double Feature - The Conversation & The 13th Floor](#) -

[SOC](#) - cont...(20:30-23:59 PDT) - [Girls Hack Village 90's House Party](#) -

[SOC](#) - cont...(20:00-21:59 PDT) - [Meet the EFF](#) -

[SOC](#) - cont...(20:00-21:59 PDT) - [Hacker Flairgrounds](#) -

[SOC](#) - cont...(20:00-21:59 PDT) - [Hacker Jeopardy](#) -

[SOC](#) - [Arcade Party](#) -

[SOC](#) - [VETCON](#) -

[SOC](#) - [Hallway Monitor Party - Entertainment](#) - Yesterday & Tomorrow,Terrestrial Access Network,Hellacopta,Hanz Dwight,DJ Thaad

## Saturday - 22:00 PDT

---

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

---

[SOC](#) - cont...(20:00-23:59 PDT) - [Movie Night Double Feature - The Conversation & The 13th Floor](#) -

[SOC](#) - cont...(20:30-23:59 PDT) - [Girls Hack Village 90's House Party](#) -

[SOC](#) - [Whose Slide Is It Anyway? \(WSIIA\)](#) -

[SOC](#) - cont...(21:00-23:59 PDT) - [Arcade Party](#) -

## Saturday - 23:00 PDT

---

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

---

SOC - cont...(20:00-23:59 PDT) - Movie Night Double Feature - The Conversation & The 13th Floor -  
SOC - cont...(20:30-23:59 PDT) - Girls Hack Village 90's House Party -  
SOC - cont...(22:00-23:59 PDT) - Whose Slide Is It Anyway? (WSIIA) -  
SOC - cont...(21:00-23:59 PDT) - Arcade Party -

---

## Sunday

---

This Schedule is tentative and may be changed at any time. Check at an Info Booth for the latest.

---

### Sunday - 09:00 PDT

---

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

---

AIV - Automate Detection with Machine Learning - Gavin Klondike  
DC - Merch (formerly swag) Area Open -- README -  
SKY - (09:30-10:20 PDT) - Eradicating Disease With BioTerrorism - Mixael S. Laufer  
SOC - Chillout Lounge - Entertainment - Merin MC,Pie & Darren,Rusty,s1gnsoflife

---

### Sunday - 10:00 PDT

---

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

---

AIV - cont...(09:00-10:20 PDT) - Automate Detection with Machine Learning - Gavin Klondike  
AIV - (10:30-11:20 PDT) - Attacks on Tiny Intelligence - Yuvaraj Govindarajulu  
ASV - Hack the Airport with Intelligenesis -  
ASV - Hack the Airfield with DDS -  
ASV - Satellite Eavesdropping with DDS -  
ASV - Self No-Fly Area Designing for UAV - Utku Yildirim  
ASV - Red Balloon Failsat Challenges -  
ASV - Hack-A-Sat Digital Twin Workshop -  
ASV - Pen Test Partners A320 Simulator -  
ASV - (10:30-11:20 PDT) - Control Acquisition Attack of Aerospace Systems by False Data Injection - Garrett Jares  
BHV - (10:30-11:59 PDT) - Memento Vivere: A connected light installation on cerebral (dys)function - Rick Martinez Herrera  
CLV - Understanding, Abusing and Monitoring AWS AppStream 2.0 - Rodrigo Montoro  
CLV - (10:40-11:20 PDT) - How to do Cloud Security assessments like a pro in only #4Steps - Ricardo Sanchez  
CPV - (10:30-10:59 PDT) - XR Technology Has 99 Problems and Privacy is Several of Them (PRE-RECORDED) - Suchi Pahi,Calli Schroeder  
DC - Human Registration Open  
DC - Vendor Area Open  
DC - cont...(09:00-14:59 PDT) - Merch (formerly swag) Area Open -- README -  
DC - Village Areas Open (Generally) -  
DDV - Last chance to pick up drives at the DDV -  
HHV - Solder Skills Village - Open  
HHV - Hardware Hacking Village - Open  
IOTV - Hands on Hardware Hacking – eMMC to Root - Deral Heiland  
IOTV - Drone Hack -

---

IOTV - IoT Village CTF -

IOTV - IoT Village CTF Challenges -

IOTV - Hands on hacking labs -

LPV - (10:15-10:45 PDT) - Intro to Lockpicking - TOOOL

PLV - Improving International Vulnerability Disclosure: Why the US and Allies Have to Get Serious - Stewart Scott,Christopher Robinson

PLV - Better Policies for Better Lives: Hacker Input to international policy challenges - Peter Stevens

SKY - cont...(09:30-10:20 PDT) - Eradicating Disease With BioTerrorism - Mixael S. Laufer

SKY - (10:35-11:25 PDT) - Basic Blockchain Forensics - K1ng\_Cr4b

SOC - cont...(09:00-14:59 PDT) - Chillout Lounge - Entertainment - Merin MC,Pie & Darren,Rusty,s1gnsofl1fe

## Sunday - 11:00 PDT

---

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

---

AIV - cont...(10:30-11:20 PDT) - Attacks on Tiny Intelligence - Yuvaraj Govindarajulu

AIV - (11:30-12:20 PDT) - AI Trojan Attacks, Defenses, and the TrojAI Competition - Taylor Kulp-Mcdowall

ASV - cont...(10:00-12:59 PDT) - Hack the Airport with Intelligenesis -

ASV - cont...(10:00-12:59 PDT) - Hack the Airfield with DDS -

ASV - cont...(10:00-12:59 PDT) - Satellite Eavesdropping with DDS -

ASV - cont...(10:00-11:59 PDT) - Red Balloon Failsat Challenges -

ASV - cont...(10:00-12:59 PDT) - Hack-A-Sat Digital Twin Workshop -

ASV - cont...(10:00-11:59 PDT) - Pen Test Partners A320 Simulator -

ASV - cont...(10:30-11:20 PDT) - Control Acquisition Attack of Aerospace Systems by False Data Injection - Garrett Jares

ASV - (11:30-11:55 PDT) - Formalizing Security Assessment for Uncrewed Aerial Systems - Rudy Mendoza,Ronald Broberg

BHV - cont...(10:30-11:59 PDT) - Memento Vivere: A connected light installation on cerebral (dys)function - Rick Martinez Herrera

BTV - Backdoors & Breaches, Back to the Stone Age! -

CLV - cont...(10:40-11:20 PDT) - How to do Cloud Security assessments like a pro in only #4Steps - Ricardo Sanchez

CLV - (11:20-11:50 PDT) - Cloud Sandboxes for Security Research - Fire from the Heavens - Louis Barrett

CLV - (11:50-12:30 PDT) - Deescalate the overly-permissive IAM - Jay Chen

CPV - Voldrakus: Using Consent String Steganography to Exfiltrate Browser Fingerprinting Data - Kaileigh McCrea

CPV - (11:30-11:59 PDT) - Finding Crypto: Inventorying Cryptographic Operations - Kevin Lai

DC - Save The Environment (Variable): Hijacking Legitimate Applications with a Minimal Footprint - Wietze Beukema

DC - STrace - A DTrace on windows reimplementaion. - Stephen Eckels

DC - cont...(10:00-15:59 PDT) - Human Registration Open

DC - Exploitation in the era of formal verification: a peek at a new frontier with AdaCore/SPARK - Adam Zabrocki,Alex Tereshkin

DC - emulation-driven reverse-engineering for finding vulns - atlas

DC - cont...(10:00-15:59 PDT) - Vendor Area Open

DC - cont...(09:00-14:59 PDT) - Merch (formerly swag) Area Open -- README -

DC - cont...(10:00-14:59 PDT) - Village Areas Open (Generally) -

HHV - cont...(10:00-12:59 PDT) - Solder Skills Village - Open

HHV - cont...(10:00-12:59 PDT) - Hardware Hacking Village - Open

HRV - Free Amateur Radio License Exams -

HRV - Oli: A Simpler Pi-Star Replacement - Danny Quist

IOTV - cont...(10:00-12:59 PDT) - Hands on Hardware Hacking – eMMC to Root - Deral Heiland

IOTV - cont...(10:00-12:59 PDT) - Drone Hack -

IOTV - cont...(10:00-12:59 PDT) - IoT Village CTF -

IOTV - cont...(10:00-12:59 PDT) - IoT Village CTF Challenges -

IOTV - cont...(10:00-12:59 PDT) - Hands on hacking labs -

LPV - Safecracking for Everyone - Jared Dygert

PLV - cont...(10:00-11:45 PDT) - Improving International Vulnerability Disclosure: Why the US and Allies Have to Get Serious - Stewart Scott,Christopher Robinson

PLV - cont...(10:00-11:45 PDT) - Better Policies for Better Lives: Hacker Input to international policy challenges - Peter

Stevens

[SKY](#) - cont...(10:35-11:25 PDT) - Basic Blockchain Forensics - K1ng\_Cr4b

[SKY](#) - (11:40-13:30 PDT) - Abortion Tech - Maggie Mayhem

[SOC](#) - cont...(09:00-14:59 PDT) - Chillout Lounge - Entertainment - Merin MC,Pie & Darren,Rusty,s1gnsofl1fe

## Sunday - 12:00 PDT

---

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

---

[AIV](#) - cont...(11:30-12:20 PDT) - AI Trojan Attacks, Defenses, and the TrojAI Competition - Taylor Kulp-Mcdowall

[AIV](#) - (12:30-13:20 PDT) - AI Village CTF Results and Q&A - Will Pearce

[ASV](#) - cont...(10:00-12:59 PDT) - Hack the Airport with Intelligenesis -

[ASV](#) - cont...(10:00-12:59 PDT) - Hack the Airfield with DDS -

[ASV](#) - cont...(10:00-12:59 PDT) - Satellite Eavesdropping with DDS -

[ASV](#) - cont...(10:00-12:59 PDT) - Hack-A-Sat Digital Twin Workshop -

[ASV](#) - Drones and Civil Liberties - Andrés Arrieta

[BHV](#) - (12:30-13:59 PDT) - In the eye of the Beholder

[BTV](#) - Project Obsidian: Panel Discussion -

[CLV](#) - cont...(11:50-12:30 PDT) - Deescalate the overly-permissive IAM - Jay Chen

[CLV](#) - (12:30-12:50 PDT) - Sign of the Times: Exploiting Poor Validation of AWS SNS SigningCertUrl - Eugene Lim

[CLV](#) - (12:50-13:30 PDT) - Cloud Defaults are Easy Not Secure - Igal Flegmann

[CPV](#) - Surviving and Designing for Survivors - Avi Zajac

[CPV](#) - (12:45-13:30 PDT) - PII: The Privacy Zombie - Alisha Kloc

[DC](#) - PreAuth RCE Chains on an MDM: KACE SMA - Jeffrey Hofmann

[DC](#) - Defaults - the faults. Bypassing android permissions from all protection levels - Nikita Kurtin

[DC](#) - cont...(10:00-15:59 PDT) - Human Registration Open

[DC](#) - The Call is Coming From Inside The Cluster: Mistakes that Lead to Whole Cluster Pwnership - Will Kline,Dagan Henderson

[DC](#) - Taking a Dump In The Cloud - Flangvik,Melvin Langvik

[DC](#) - cont...(10:00-15:59 PDT) - Vendor Area Open

[DC](#) - cont...(09:00-14:59 PDT) - Merch (formerly swag) Area Open -- README -

[DC](#) - cont...(10:00-14:59 PDT) - Village Areas Open (Generally) -

[HHV](#) - cont...(10:00-12:59 PDT) - Solder Skills Village - Open

[HHV](#) - cont...(10:00-12:59 PDT) - Hardware Hacking Village - Open

[HRV](#) - cont...(11:00-13:59 PDT) - Free Amateur Radio License Exams -

[HRV](#) - (12:30-12:59 PDT) - Off the grid - Supplying your own power - Eric Escobar

[IOTV](#) - cont...(10:00-12:59 PDT) - Hands on Hardware Hacking - eMMC to Root - Deral Heiland

[IOTV](#) - cont...(10:00-12:59 PDT) - Drone Hack -

[IOTV](#) - cont...(10:00-12:59 PDT) - IoT Village CTF -

[IOTV](#) - cont...(10:00-12:59 PDT) - IoT Village CTF Challenges -

[IOTV](#) - cont...(10:00-12:59 PDT) - Hands on hacking labs -

[LPV](#) - Doors, Cameras, and Mantraps. Oh, my! - Dylan Baklor

[PLV](#) - Offensive Cyber Industry Roundtable - Sophia D'Antoine,Winnona DeSombre,Matt Holland

[PLV](#) - Protect Our Pentest Tools! Perks and Hurdles in Distributing Red Team Tools -

[SKY](#) - cont...(11:40-13:30 PDT) - Abortion Tech - Maggie Mayhem

[SOC](#) - cont...(09:00-14:59 PDT) - Chillout Lounge - Entertainment - Merin MC,Pie & Darren,Rusty,s1gnsofl1fe

[SOC](#) - Friends of Bill W -

## Sunday - 13:00 PDT

---

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

---

[AIV](#) - cont...(12:30-13:20 PDT) - AI Village CTF Results and Q&A - Will Pearce

[BHV](#) - cont...(12:30-13:59 PDT) - In the eye of the Beholder

BTV - Blue Team Village Closing Ceremony -  
CLV - cont...(12:50-13:30 PDT) - Cloud Defaults are Easy Not Secure - Igal Flegmann  
CLV - (13:30-13:45 PDT) - [Cloud Village Closing Note](#) - Jayesh Singh Chauhan  
CPV - cont...(12:45-13:30 PDT) - PII: The Privacy Zombie - Alisha Kloc  
CPV - (13:30-14:15 PDT) - [Cryptosploit](#) - Matt Cheung,Benjamin Hendel  
DC - ElectroVolt: Pwning popular desktop apps while uncovering new attack surface on Electron - Max Garrett,Aaditya Purani  
DC - The Journey From an Isolated Container to Cluster Admin in Service Fabric - Aviv Sasson  
DC - cont...(10:00-15:59 PDT) - Human Registration Open  
DC - Less SmartScreen More Caffeine – ClickOnce (Ab)Use for Trusted Code Execution - Nick Powers,Steven Flores  
DC - TBA - Benny Zeltser  
DC - RingHopper – Hopping from User-space to God Mode - Jonathan Lusky,Benny Zeltser  
DC - cont...(10:00-15:59 PDT) - Vendor Area Open  
DC - cont...(09:00-14:59 PDT) - [Merch \(formerly swag\) Area Open -- README](#) -  
DC - cont...(10:00-14:59 PDT) - [Village Areas Open \(Generally\)](#) -  
HRV - cont...(11:00-13:59 PDT) - Free Amateur Radio License Exams -  
LPV - [Intro to Lockpicking](#) - TOOOL  
PLV - cont...(12:00-13:45 PDT) - Offensive Cyber Industry Roundtable - Sophia D'Antoine,Winnona DeSombre,Matt Holland  
PLV - cont...(12:00-13:45 PDT) - Protect Our Pентest Tools! Perks and Hurdles in Distributing Red Team Tools -  
SKY - cont...(11:40-13:30 PDT) - [Abortion Tech](#) - Maggie Mayhem  
SOC - cont...(09:00-14:59 PDT) - [Chillout Lounge - Entertainment](#) - Merin MC,Pie & Darren,Rusty,s1gnsof11fe

## Sunday - 14:00 PDT

---

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

---

AIV - AI Village Closing Remarks - Sven Cattell,Brian Pendleton  
CPV - cont...(13:30-14:15 PDT) - [Cryptosploit](#) - Matt Cheung,Benjamin Hendel  
CPV - (14:15-14:59 PDT) - [AES-GCM common pitfalls and how to work around them \(PRE-RECORDED\)](#) - Santiago Kantorowicz  
DC - Contest Closing Ceremonies & Awards - Grifter  
DC - Solana JIT: Lessons from fuzzing a smart-contract compiler - Thomas Roth  
DC - cont...(10:00-15:59 PDT) - Human Registration Open  
DC - cont...(10:00-15:59 PDT) - Vendor Area Open  
DC - cont...(09:00-14:59 PDT) - [Merch \(formerly swag\) Area Open -- README](#) -  
DC - cont...(10:00-14:59 PDT) - [Village Areas Open \(Generally\)](#) -  
LPV - [The "Why" of Lock Picking](#) - Christopher Forte (isaidnocookies)  
SOC - cont...(09:00-14:59 PDT) - [Chillout Lounge - Entertainment](#) - Merin MC,Pie & Darren,Rusty,s1gnsof11fe

## Sunday - 15:00 PDT

---

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

---

DC - cont...(14:00-15:15 PDT) - [Contest Closing Ceremonies & Awards](#) - Grifter  
DC - cont...(10:00-15:59 PDT) - Human Registration Open  
DC - (15:30-17:30 PDT) - [DEF CON Closing Ceremonies & Awards](#) - The Dark Tangent  
DC - cont...(10:00-15:59 PDT) - Vendor Area Open

## Sunday - 16:00 PDT

---

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

---

## Sunday - 17:00 PDT

---

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

---

DC - cont...(15:30-17:30 PDT) - DEF CON Closing Ceremonies & Awards - The Dark Tangent

---

## Speaker List

---

3ncr1pt3d

A.Krontab

Aaditya Purani

Aakinn Patel

Aaron DeVera

Aaron Rosenmund

Abdul Alanazi

Abhinav Singh

Abhinav Singh

Adam Dobell

Adam Dobell

Adam Hickey

Adam Hickey

Adam Zabrocki

Adrian Wood

Adrien Ogee

Adrien Ogee

AJ King

Alberto Herrera

Alex Lomas

Alex Tereshkin

Alexandre Sieira

Alexandrine Torrents

Alexandrine Torrents

Alexis Goldstein

Alexis Hancock

Alisha Kloc

Alison N

Alison N

Alissa Knight

Alissa Torres

Andrés Arrieta

Andrea Downing

Andrea Downing

Andres Meza

Andrew Green

Andrew Klein

Andrew Logan

Ankur Tyagi

Anthony "Cx01N" Rose

Anthony "Cx01N" Rose

Anthony Hendricks

Anton Ovrutsky

Apurv Singh Gautam

Archwisp

Arik

Arikia Millikan

Arikia Millikan

Arnaud Soullie

Arnaud Soullie

Asaf Gilboa

Ashlee Benge

atlas

Aubrey Labuschagne (William)

Aubrey Labuschagne (William)

Audrey Dutcher

Audrey Dutcher

Avi Zajac

Avi Zajac

aviditas

aviditas

aviditas

Aviv Sasson

Ayan Islam

Ayan Islam

Barrett Darnell

Ben Barnea

Ben Gardiner

Ben Gelman

Ben Hawks

Ben Hughes

Ben Kurtz

Benjamin Hendel

Benny Zeltser

Benny Zeltser

Berkelly Gonzalez

Bill Graydon

Billy Jheng

Biolux

Birhanu Eshete

Bradán Lane

Brandon Bailey

Brandon Enright

Brenton Morris

Brian Pendleton

Brian Pendleton

Bryan C. Geraghty

Bryson Bort

burninator

Calli Schroeder

Cam

CaptHz

Carey Parker

Carlos Galán

Carson Zimmerman

Cassandra Bailey

Cassandra Young (muteki)

Cassandra Young (muteki)

CerealKiller

Cesare Pizzi

Ch33r10

Cheryl Biswall

ChocolateCoat

ChocolateCoat

ChocolateCoat

Chris Forte

Chris Greer

Chris Greer

Chris Kubecka

Chris Kubecka

Chris Poore

Chris Rock

Chris Thompson

Christian "quaddi" Dameff MD

Christian "quaddi" Dameff MD

Christophe Tafani-Dereeper

Christopher Forte (isaidnocookies)

Christopher Panayi

Christopher Poore

Christopher Robinson

CISA Staff

CodexMafia

Cody Wayne Burkhart

ColdwaterQ

Connor Morley

Cory Doctorow

Corynne McSherry

CountZ3r0

CountZ3r0

CountZ3r0

CTRL/rsm

Cyb3rHawk

dadabots

Dagan Henderson

Dahvid Schloss

Dahvid Schloss

Damian Grant

Dan Nagle

Daniel Chen

Daniel Crowley

Daniel Jensen

Daniel Prizmant

Danny D. Henderson Jr (B4nd1t0)

Danny Quist

Darwin Salazar

David Brearley

David Forscley

David McGrew

David Mitchell

Dazza Greenwood

DEF CON Goons

DEF CON Policy Dept  
Deneen Defiore  
Deral Heiland  
Deral Heiland  
Deral Heiland  
Deviant Ollam  
DHS Staff  
Dikla Barda  
DJ Scythe  
DJ St3rling  
DJ Thaad  
DJ UNIT 77 [ 0077 : 0077 ]  
djdead  
djdead  
djdead  
Dominic "Cryillic" Cunningham  
Dongsung Kim  
DotOrNot  
Dr. Amanda Minnich  
Dr. Bramwell Brizendine  
Dr. Josef Schmid  
Dr. McGrew  
Dr. Meisam Eslahi  
Dual Core  
Duane Michael  
Dylan Baklor  
Eigentourist  
Elijah  
Eirick Luraas  
Eirick Luraas  
Elizabeth Biddlecome  
Elizabeth Biddlecome  
Emma Best  
Eran Segal  
Eric Escobar  
Eric Escobar  
Eric Mair  
Eric Mill  
Erica Burgess  
Erie Meyer  
Esther Matut  
Eugene Lim  
Eugene Lim  
ExtremePaperClip  
ExtremePaperClip  
ExtremePaperClip  
ExtremePaperClip  
Eytan Tepper  
Felipe Espósito  
Fernando Perera

Filipi Pires  
Fish Wang  
Fish Wang  
Flangvik

Florian Lukavsky  
Four Thieves Vinegar Collective

FuzzyNop  
Göktay Kaykusuz

GACWR Team  
GACWR Team

Gadi Evron  
Gal Sadeh

Gal Zror

Game Tech Chris

Garrett Jares

Gauthier Sebaux

Gavin Klondike

Gavin Klondike

Georges-Axel Jaloyan

Gilmar Esteves

Gina Rosenthal

Ginny Fahs

Gonzalo Munilla Garrido

Griffin Francis

Grifter

Guillaume Ross

Guy Barnhart-Magen

Hadrien Barral

Hanz Dwight

Hardik Shah

Harini Kannan

Harley Geiger

Harri Hursti

Harry Mourtos

Heckseven

Hellacopta

Henry Haswell

Hyrum Anderson

Ian Vitek

Ictre Normal

ICSNick - Nicklas Keijser

Igal Flegmann

Ionut Cernica

Irene Mo

Irfan Hemani

Irfan Hemani

Irvin Lemus

Irvin Lemus

Isabel Straw

Jack Cable

Jack Cable

Jackie Bow

Jacob Baines

Jake "Hubbl3" Krasnov

Jake Labelle

Jake Labelle

Jake Williams

James Kettle

James Pavur

James Pavur

Jamie Williams

Jamie Williams

Jared Dygert

Jason Healey

Jason Johnson

Jay Chen

Jay Chen

Jay Lagorio

Jayesh Singh Chauhan

Jayesh Singh Chauhan

Jeff "r3plicant" Tully MD

Jeff "r3plicant" Tully MD

Jeffrey Hofmann

Jen Ellis

Jen Ellis

Jenko Hwong

Jenna Sherman

Jennifer Mathieu

Jennifer Mathieu

Jeremy Hong

Jeremy Linden

Jeremy Miller

Jeremy Miller

Jess

Jesse Michael

Jessica Dheere

Jessica Wilkerson

Jeswin Mathai

Jeswin Mathai

Ji Su Yoo

Jillian Simons

Jimi Allee

Jimmy Wylie

Jivesx

Joe Grand

Joe Schottman

Joe Slowik

John Midgley

John Orleans

Jon Christiansen

Jon Marler

Jonathan Fischer

Jonathan Fischer

Jonathan Leitschuh

Jonathan Lusky

Jonathan Tomek

Jonghyuk Song

Jorge Acevedo Canabal

Jose Pico

Jose Pizarro

Joseph Ravichandran

Josh Stroschein

Jovonni Pharr

Jovonni Pharr

Judge Taylor

juju43

juju43

Junyuan Zeng

Justin Elze

Justin Gardner

Justin Hutchens

Justin Rhinehart

Justin/InkRF

K1ng\_Cr4b

Kaileigh McCrea

Kaitlyn Handleman

Kaitlyn Handleman

Kampf

Kampf

Kampf

Kamron Talebzadeh

Karl Fosaaen

Karl Koscher

Kassandra Pierre

Kat Fitzgerald

Kate Bertash

Kathy Satterlee

Katie Whiteley (Mkfactor)

Keith E. Sonderling

Keith Meyers

Ken Gannon

Ken Johnson

Ken Johnson

Ken Munro

Ken Munro

Ken Pyle

Kenneth Geers

Kenzie Dolan

Kevin Clark

Kevin Lai

Kimberly Mentzell

Kostas

Kristen Cotten

Krisz Klink

Kyle Avery

Kyle Wiens

KyleHaxWhy

l00sid

l00sid

l0ngrange

Larsbodian

Larsbodian

Laura Whitt-Winyard

Lauren Proehl

Lennert Wouters

Leo Nendza

Leonard Bailey

Levone Campbell

Lior Kolnik

LitMoose

Logan Arkema

Louis Barrett

Louis Rossmann

Lucas Bonastre

Luke Richards

Madhu Akula

Madhu Akula

Maggie Mayhem

Magician Kody Hildebrand

Magician Kody Hildebrand

Magician Kody Hildebrand

Magik Plan

Magnus Stubman

Malcolm Galland

Mariam Elgabry

Marianka Botes

Marianka Botes

Mark Morowczynski

Martin Doyhenard

Mary Brooks

Mass Accelerator

Matt Cheung

Matt Cheung

Matt Holland

Matt Mosley

Matt Nash

Matt Scheurer

Matthew Canham

Matthew Guariglia

Matthew Handy

Mauricio Tavares

Mauricio Velazco

Max Garrett

Maxime Meignan

Maxwell Dulin

Meg King

Melvin Langvik

Merin MC

Merin MC

Merin MC

Merin MC

Miana E Windall

Michael Aguilar (v3ga)

Michael Bargury

Michael Bargury

Michael Epping

Michael Messner

Michael Pelosi

Michael Register

Michael Ross

DEFCON

Michael Solomon

Michael Whiteley (Mkfactor)

Mickey Shkatov

Micsen

Mike Campanelli

Mike Guirao

Mike Kijewski

Mike Mittelman

Minh Duong

Miss Jackalope

Misstech

Mixael S. Laufer

Mixael S. Laufer

Moritz Abrell

Muhammad ALifa Ramdhani

Musaed Bin Muatred

n0x08

N\_thing

N\_thing

nas\_bench - Nasreddine Bencherchali

Nathan Case

Nathan Chung

Nathan Kirkland

Nathaniel Quist

Neal Pollard

Nestori Syynimaa

Nestori Syynimaa

Neumann Lim (scsideath)

Nevada Romsdahl

Nicholas Coad

Nicholas Coad

Nick Ascoli

Nick Baker

Nick Dorion

Nick Gobern

Nick Powers

Nick Vidal

Nick Vidal

Nicole Chi

Nikita Kurtin

Nina Alli

Nina Kollars

Nishant Sharma

Nishant Sharma

Noam Dahan

Noam Dahan

Noam Dahan

nohackme

NPC Collective

Ochuan Marshall

Octavio Galland

Octavio Gianatiempo

Oded Vanunu

Ohad Zaidenberg

Olaf Hartong

Olivia Stella  
Omenscan  
Omenscan  
Omenscan  
Omenscan  
Omenscan  
Omri Misgav  
Ophir Harpaz  
Orange Tsai  
p80n  
PankleDank

Pascal Eckmann

Patrick McNeil

Patrick Ross

Patrick Ross

Patrick Wardle

Patrick Wardle

Paul Flynn

Paul Laîné

Paul Roberts

Paul Young

Paula González Nagore

Per Thorsheim

Pete Cooper

Peter Stevens

Phil Young

Philippe Laulheret

Pie & Darren

Pie & Darren

Pie & Darren

Pie & Darren

plug

Preslav Nakov

Preslav Nakov

Quentin Kaiser

r3c0d3

Rachna Umraニーा

Raunak Parmar

Ray "Senpai" Morris

Rebecca Ash

Remi Escourrou

Rex Guo

Rhyner Washburn

Ricardo Sanchez

Ricardo Sanchez

Ricardo Sanchez

Rich

Richard Thieme

Richard Thieme

Richard Zak

Richard Zak

Rick Martinez Herrera

Rick Osgood

Rick White

Ricky Banda

Rishal Dwivedi  
Robert Fitzpatrick  
Rodrigo Montoro  
Roger Dingledine  
Rohan Durve  
Roman Zaikin  
Ron Ben Yitzhak  
Ronald Broberg  
Ronny Thammashithi  
Roy Stultiens  
Rudy Mendoza  
Russ Handorf  
Rusty  
Rusty  
Rusty  
Rusty  
Ryan Ashley  
Ryan J Chapman  
Ryan Kovar  
Ryan Rix  
Ryan Westman  
s1gns0f1fe  
s1gns0f1fe  
s1gns0f1fe  
s1gns0f1fe  
Safa Shahwan Edwards  
Salma Taoufiq  
Sam Bent  
Sam Bowne  
Sam Bowne  
Sam Curry  
Sam Quinn  
Samuel Erb  
SamunoskeX  
Sanjeev Mahunta  
Santiago Kantorowicz  
Santiago Kantorowicz  
Sara-Jayne Terp  
Sarthak Taneja  
Saurabh Chaudhary  
Scotch and Bubbles  
Scott Small  
Sean Sullivan  
Sean Wilson  
Sean Zadig  
Sebastian Stein  
Seeyew Mo  
Segun Ebenezer Olaniyan  
Seongsu Park  
Sergei Frankoff  
Seth Kintigh  
Seth Law  
Seth Law  
Shannon McHale  
Sharon Brizinov

Shawn Thomas  
Sherrod DeGrippo  
Shubham Dubey  
Sick Codes  
Siebren Kraak  
Skittish & Bus  
Slava Makkaveev  
Solomon Sonya  
Solomon Sonya  
Soohwan Oh  
Sophia D'Antoine  
Spicy Wasabi  
stacksmashing  
Stephanie Barnes  
Stephanie G.  
Stephanie G.  
Stephen Eckels  
Stephen Kofi Asamoah  
Steve Povolny  
Steve Thomas  
Steven Collins  
Steven Flores  
Stewart Scott  
Stewart Scott  
Suchi Pahi  
Sudipto Rakshit  
Sven Cattell  
Sven Cattell  
Swapneel Mehta  
TAIKOPROJECT  
Tanisha O'Donoghue  
Tarek Abdelmotaleb  
Tavoo  
Taylor Kulp-Mcdowall  
Tense Future  
Teresa Merklin  
Terrestrial Access Network  
The Dark Tangent  
The Dark Tangent  
The Dark Tangent  
Thijs Alkemade  
Thomas Diot  
Thomas Roth  
Timothy Weston  
Timothy Weston  
Tom Dohrmann  
Tom McGuire  
Tomer Bar  
Toni de la Fuente  
TOOOL  
TOOOL  
TOOOL  
TOOOL  
TOOOL

TOOOL

TOOOL

Tracy Z. Maleeff

Trevor Hough

Trevor Hough

Trevor Stevado

Trevor Stevado

Trevor Timmons

Trey Herr

Trey Herr

TRIODE

Tristan Miller

ttheveii0x

ttheveii0x

Uchi Uchibeke

Uchi Uchibeke

Ulf Frisk

Utku Yildirim

Valencia Robinson

Valencia Robinson

Victor Graf

Vincent "Vinnybod" Rose

Vincent "Vinnybod" Rose

Vivek Nair

Vivek Nair

Wes Gavins

Wes Lambert

Wes Lambert

Wesley Thurner

Whitney Merrill

Wietze Beukema

Will Kline

Will Pearce

Winn Schwartau

Winnona DeSombre

Winnona DeSombre

Woongjo choi

Xan North

Xavier Gerondeau

Yael Grauer

Yesterday & Tomorrow

Yolan Romailler

Ytcracker

Yuvaraj Govindarajulu

Z3NPI

Zachary Minneker

Zachary Minneker

Zebbler Encanti Experience

Zhouhan Chen

zr0

DEFCON

DEFCON

# Talk List

---

- "The Man" in the Middle - BICV  
[T]OTPs are not as secure as you might believe - CPV  
404! Memory Holing and the SEO Warping of Human History - MIV  
A Capitalist approach to hospital security - BHV  
A dead man's full-yet-responsible-disclosure system - DC  
A few useful things to know about AI Red Teams - AIV  
A Practical Approach to Breaking & Pwning Kubernetes Clusters - PT  
A Practical Approach to Breaking & Pwning Kubernetes Clusters - PT  
A ransomware actor looks at the clouds: attacking in a cloud-native way - CLV  
A System for Alert Prioritization - AIV  
AADInternals: The Ultimate Azure AD Hacking Toolkit - DL  
Abortion Tech - SKY  
Access Undenied on AWS - Troubleshooting AWS IAM AccessDenied Errors - CLV  
Access Undenied on AWS - DL  
Ad it up: To minimize mis- and dis-information, we must reshape the ad tech business, not regulate speech - MIV  
Addressing the gap in assessing (or measuring) the harm of cyberattacks - PLV  
AES-GCM common pitfalls and how to work around them (PRE-RECORDED) - CPV  
AI Music Tutorial and Show - AIV  
AI Trojan Attacks, Defenses, and the TrojAI Competition - AIV  
AI Village Closing Remarks - AIV  
AI Village CTF Results and Q&A - AIV  
AI Village Keynote - AIV  
All information should be free (except the brain data you want to keep in your head) - BHV  
All Roads leads to GKE's Host : 4+ Ways to Escape - DC  
alsanna - DL  
Amazon Web Services Aerospace and Satellite Jam - ASV  
Amazon Web Services Aerospace and Satellite Jam - ASV  
Analyzing PIPEDREAM: Challenges in testing an ICS attack toolkit. - DC  
Android, Birthday Cake, Open Wifi... Oh my! - SKY  
Arcade Party - SOC  
Ask an Airport CISO - ASV  
Attacks on Tiny Intelligence - AIV  
Attribution and Bias: My terrible mistakes in threat intelligence attribution - BTV  
Automate Detection with Machine Learning - AIV  
Automate Detection with Machine Learning - AIV  
Automated Debugging Under The Hood - Building A Programmable Windows Debugger From Scratch (In Python) - WS  
Automated Trolling for Fun and No Profit - SKY  
Automating Insecurity in Azure - CLV  
Automotive Ethernet Fuzzing: From purchasing ECU to SOME/IP fuzzing - DC  
Avoiding Memory Scanners: Customizing Malware to Evade YARA, PE-sieve, and More - DC  
AWSGoat : A Damn Vulnerable AWS Infrastructure - DL  
AzureGoat: Damn Vulnerable Azure Infrastructure - DL  
Back to School! Hello RSA... and beyond! - CPV  
Backdooring Pickles: A decade only made things worse - DC  
Backdoors & Breaches, Back to the Stone Age! - BTV  
Badrats: Initial Access Made Easy - DL  
Basic Blockchain Forensics - SKY  
Better Policies for Better Lives: Hacker Input to international policy challenges - PLV  
BioHacking Village Keynote - BHV  
Black & White Ball - Entertainment - SOC  
Black-Box Assessment of Smart Cards - DC  
BlanketFort Con - SOC

Blue Team Village Closing Ceremony - BTV  
Blue Team Village Opening Ceremony - BTV  
Blue Teaming Cloud: Security Engineering for Cloud Forensics & Incident Response - BTV  
BlueTeam Village Party - SOC  
Boeing ARINC 429 Airplane Challenge and CTF - ASV  
Boeing ARINC 429 Airplane Challenge and CTF - ASV  
Brazil Redux: Short Circuiting Tech-Enabled Dystopia with The Right to Repair - DC  
Breaking the Intelligence Cycle - how to tailor intelligence function to your needs? - BHV  
BrokenbyDesign: Azure | Get started with hacking Azure - CLV  
Browser-Powered Desync Attacks: A New Frontier in HTTP Request Smuggling - DC  
Building Your Own Satellite Ground Station - ASV  
BURP Suite, Forensics Tools & 0-day Exploit Development. - IOTV  
California CyberSecurity Institute Space Grand Challenge - ASV  
Call for Evidence: Informing the Biological Security Strategy - BHV  
Capturing Chaos: Harvesting Environmental Entropy - CPV  
CatPhish Automation - The Emerging Use of Artificial Intelligence in Social Engineering - AIV  
Challenges in Control Validation - BTV  
Chillout Lounge - Entertainment - SOC  
Chromebook Breakout: Escaping Jail, with your friends, using a Pico Ducky - DC  
CICD security: A new eldorado - WS  
Cloud Defaults are Easy Not Secure - CLV  
Cloud Sandboxes for Security Research - Fire from the Heavens - CLV  
Cloud Threat Actors: No longer cryptojacking for fun and profit - SKY  
Cloud Village Closing Note - CLV  
Cloud Village Opening Note - CLV  
Cognitive Security in Theory and Practice - MIV  
Cognitive Security: Human Vulnerabilities, Exploits, & TTPs - MIV  
Combatting sexual abuse with threat intelligence techniques - SKY  
Coming Home to Def Con: A Deep Dive into the Real Essence and Ethos of Hacking - SKY  
Computer Hacks in the Russia-Ukraine War - DC  
Confessions of a CISO - SKY  
Confronting Reality in Cyberspace: Foreign Policy for a Fragmented Internet - PLV  
Contest Closing Ceremonies & Awards - DC  
Control Acquisition Attack of Aerospace Systems by False Data Injection - ASV  
Control Validation Compass – Threat Modeling Aide & Purple Team Content Repo - DL  
Creating and uncovering malicious containers. - WS  
Creating More Black Hackers: Growth Systems for Cybersecurity Enthusiasts - BICV  
Crossing the KASM -- a webapp pentest story - DC  
Cryptle: a secure multi-party Wordle clone with Enarx - CPV  
Cryptocurrency: A Bridge Across the Digital Divide - BICV  
Cryptosploit - CPV  
CTF 101: Breaking into CTFs (or “The Petting Zoo” - Breaking into CTFs) - WS  
Customizable Binary Analysis: Using angr to its full potential - PT  
Customizable Binary Analysis: Using angr to its full potential - PT  
Cyber Star Card Game Tutorial - ASV  
Cyber Star© Competition Presented by The Space ISAC - ASV  
Cyber Threats Against Aviation Systems: The Only Threat Briefing You Really Need - ASV  
CyberPeace Builders - DL  
Déjà Vu: Uncovering Stolen Algorithms in Commercial Products - DC  
Dancing Around DRM - SKY  
Dazed and Seriously Confused: Analysis of Data Voids & the Disinformation Landscape of Central Asia - MIV  
DC404/DC678/DC770/DC470 (Atlanta Metro) Meetup - SOC

DC702 Pwnagotchi Party - SOC

DDS Space Signal Lab - ASV

DDV open and accepting drives for duplication - DDV

DDV open and accepting drives for duplication - DDV

DDV starts accepting drives for duplication - DDV

Deadly Russian Malware in Ukraine - SKY

Deanonymization of TOR HTTP hidden services - DC

Decolonizing Cybersecurity - BICV

Deescalate the overly-permissive IAM - CLV

DEF CON Bike Ride "CycleOverride" - SOC

DEF CON Closing Ceremonies & Awards - DC

DEF CON Holland DC3115 & DC3120 Group Meetup - SOC

DEF CON Policy Dept - Special Edition Policy Talk - DC

DEF CON Policy Dept - Special Edition Policy Talk - DC

DEF CON Policy Dept - Special Edition Policy Talk - DC

DEF CON Policy Dept - Special Edition Policy Talk - DC

DEF CON Policy Dept - Special Edition Policy Talk - DC

DEF CON Policy Dept - Special Edition Policy Talk - DC

Defaults - the faults. Bypassing android permissions from all protection levels - DC

Defeating Moving Elements in High Security Keys - DC

Defender's Guide to Securing Public Cloud Infrastructures - PT

Defender's Guide to Securing Public Cloud Infrastructures - PT

Defense Through a TAC (Technical Advisory Committee) - PLV

Defensive 5G - DL

DEI in Cybersecurity (Breaking through the barrier, behind the barrier... behind the barrier) - BICV

Denial, Deception, and Drinks with Mitre Engage - SOC

Department of Defense 5G Telemedicine and Medical Training: The Future of Healthcare the Remote Warrior - BHV

Detecting the "Fake News" Before It Was Even Written, Media Literacy, and Flattening the Curve of the COVID-19

Infodemic - MIV

DFIR Against the Digital Darkness: An Intro to Forensicking Evil - WS

Dig Dug: The Lost Art of Network Tunneling - WS

Digging into Xiaomi's TEE to get to Chinese money - DC

Digital Skeleton Keys - We've got a bone to pick with offline Access Control Systems - DC

DIY Medicine With Unusual Uses for Existing FDA-Approved Drugs - BHV

DIY MQTT IoT (or how you can turn your home into an interconnected palace of human-centric data) - BHV

Do No Harm (Lounge) - PLV

Do Not Trust the ASA, Trojans! - DC

Doing the Impossible: How I Found Mainframe Buffer Overflows - DC

Don't Blow A Fuse: Some Truths about Fusion Centres - SKY

Doors, Cameras, and Mantraps. Oh, my! - LPV

Dragon Tails: Supply-side Security and International Vulnerability Disclosure Law - DC

Drone Hack - IOTV

Drone Hack - IOTV

Drone Hack - IOTV

Drones and Civil Liberties - ASV

EDR detection mechanisms and bypass techniques with EDRSandBlast - DL

EFF Tech Trivia - SOC

EFF: Reproductive Justice in the Age of Surveillance - SOC

Election Security Bridge Building - PLV

ElectroVolt: Pwning popular desktop apps while uncovering new attack surface on Electron - DC

EMBA - Open-Source Firmware Security Testing - DL

Emoji Shellcoding: , , and - DC

Empire 4.0 and Beyond - DL

emulation-driven reverse-engineering for finding vulns - DC

Eradicating Disease With BioTerrorism - SKY

Ethical considerations in using digital footprints for verifying identities for online services - RHV

Evading Detection: A Beginner's Guide to Obfuscation - WS

Even my Dad is a Threat Modeler! - BTV

Examining the urgency of gendered health misinformation online through three case studies - MIV

Exploitation in the era of formal verification: a peek at a new frontier with AdaCore/SPARK - DC

Exploring Ancient Ruins to Find Modern Bugs: Discovering a 0-Day in an MS-RPC Service - DC

Exploring the hidden attack surface of OEM IoT devices: pwning thousands of routers with a vulnerability in Realtek's SDK for eCos OS. - DC

Exploring Unprecedented Avenues for Data Harvesting in the Metaverse - CPV

Faking Positive COVID Tests - BHV

FARA and DOJ's Approach to Disinformation - MIV

Final Boarding Call for Cyber Policy Airlines Flight 443 - ASV

Finding Crypto: Inventorying Cryptographic Operations - CPV

Finding Security Vulnerabilities Through Fuzzing - WS

Fireside Chat - MIV

Fireside Chat - MIV

FISSURE: The RF Framework - DL

Flying Under Cloud Cover: Built-in Blind Spots in Cloud Security - CLV

Formalizing Security Assessment for Uncrewed Aerial Systems - ASV

Free Amateur Radio License Exams - HRV

Free Amateur Radio License Exams - HRV

Free Amateur Radio License Exams - HRV

Friends of Bill W - SOC

FROM ZERO TO HERO IN A BLOCKCHAIN SECURITY - WS

From Zero To Sao ... Or, How Far Does This Rabbit Hole Go? - HHV

Fun with Factoring Large Prime Numbers - CPV

Generative Art Tutorial - AIV

Getting on the air: My experiences with Ham radio QRP - HRV

Gird your loins: premise and perils of biomanufacturing - BHV

Girls Hack Village 90's House Party - SOC

Girls Hack Village Meetup - SOC

Glitched on Earth by humans: A Black-Box Security Evaluation of the SpaceX Starlink User Terminal - DC

GOTHCON (#DCGOTHCON) - SOC

Hack the Airfield with DDS - ASV

Hack the Airfield with DDS - ASV

Hack the Airfield with DDS - ASV

Hack the Airport with Intelligenesis - ASV

Hack the Airport with Intelligenesis - ASV

Hack the Airport with Intelligenesis - ASV

HACK THE HEMISPHERE! How we (legally) broadcasted hacker content to all of North America using an end-of-life geostationary satellite, and how you can set up your own broadcast too! - DC

Hack-A-Sat Aerospace PiSat Challenge - ASV

Hack-A-Sat Aerospace PiSat Challenge - ASV

Hack-A-Sat Digital Twin Workshop - ASV

Hack-A-Sat Digital Twin Workshop - ASV

Hack-A-Sat Digital Twin Workshop - ASV

Hack-A-Sat Team - ASV

Hacker Flairgrounds - SOC

Hacker Jeopardy - SOC

Hacker Jeopardy - SOC

Hacker Karaoke - SOC  
Hacker Karaoke - SOC  
Hackers Help Make My Airline Secure - ASV  
Hacking Aviation Policy - PLV  
Hacking Ham Radio: Dropping Shells at 1200 Baud - HRV  
Hacking Hashcat - PWV  
Hacking ISPs with Point-to-Pwn Protocol over Ethernet (PPPoE) - DC  
Hacking law is for hackers - how recent changes to CFAA, DMCA, and global policies affect security research - PLV  
Hacking Operational Collaboration - PLV  
Hacking Product Security Interviews - IOTV  
Hacking Product Security Interviews - IOTV  
Hacking The Farm: Breaking Badly Into Agricultural Devices. - DC  
Hacking the Metal 2: Hardware and the Evolution of C Creatures - WS  
Hallway Monitor Party - Entertainment - SOC  
Hallway Monitor Party - Entertainment - SOC  
Hallway Monitor Party - Entertainment - SOC  
Ham Nets 101 - HRV  
Hand On Mainframe Buffer Overflows - RCE Edition - WS  
Handcuffs and how they work - LPV  
Hands on hacking labs - IOTV  
Hands on hacking labs - IOTV  
Hands on hacking labs - IOTV  
Hands on Hardware Hacking – eMMC to Root - IOTV  
Hands on Hardware Hacking – eMMC to Root - IOTV  
Hands on Hardware Hacking – eMMC to Root - IOTV  
Hands-on Hacking of Reinforcement Learning Systems - AIV  
Hands-On TCP/IP Deep Dive with Wireshark - How this stuff really works - WS  
Heavyweights: Threat Hunting at Scale - BTV  
History of Russian Cyber & Information Warfare (2007-Present) - MIV  
History of the weaponization of social media - MIV  
hls4ml - Open Source Machine Learning Accelerators on FPGAs - DL  
Horusec - Brazilian SAST help World - BTV  
House of Heap Exploitation - WS  
How long do hard drives and SSDs live, and what can they tell us along the way? - DDV  
How Russia is trying to block Tor - DC  
How to Build DIY Lifesaving Medical Devices - BHV  
How to do Cloud Security assessments like a pro in only #4Steps - CLV  
How To Get MUMPS Thirty Years Later (or, Hacking The Government via FOIA'd Code) - DC  
How to Leverage MDS2 Data for Medical Device Security - BHV  
How to Respond to Data Subject Access Requests - CPV  
How to stop Surveillance Capitalism in Healthcare - BHV  
Hundreds of incidents, what can we share? - SKY  
Hunting Bugs in The Tropics - DC  
Hunting for Spacecraft Zero Days Using Digital Twins - ASV  
Hunting Malicious Office Macros - BTV  
Hybrid Phishing Payloads: From Threat-actors to You - WS  
I'm not Keylogging you! Just some benign data collection for User Behavior Modeling - AIV  
ID theft insurance - The Emperor's new clothes? - CPV  
Imagining a cyber policy crisis: Storytelling and Simulation for real-world risks - PLV  
Improving International Vulnerability Disclosure: Why the US and Allies Have to Get Serious - PLV  
Improving security posture of MacOS and Linux with Azure AD - BTV  
Information Confrontation 2022 - A loud war and a quiet enemy - MIV  
Injectyll-Hide: Build-Your-Own Hardware Implants - HHV  
Injectyll-HIDE: Pushing the Future of Hardware Implants to the Next Level - DL  
Internal Server Error: Exploiting Inter-Process Communication with new desynchronization primitives - DC

International Government Action Against Ransomware - PLV  
INTERNET WARS 2022: These wars aren't just virtual - SKY  
Intro to Lockpicking - LPV  
Introducing the Abusability Testing Framework (V1) - CPV  
Introduction to Aircraft Networks and Security Design Considerations - ASV  
Introduction to Azure Security - WS  
Introduction to Cryptographic Attacks - WS  
Introduction to Software Defined Radios and RF Hacking - WS  
IoT Village CTF Challenges - IOTV  
IoT Village CTF Challenges - IOTV  
IoT Village CTF Challenges - IOTV  
IoT Village CTF Creator's Contest - IOTV  
IoT Village CTF - IOTV  
IoT Village CTF - IOTV  
IoT Village CTF - IOTV  
Jailed By a Google Search Part 2: Abortion Surveillance in Post-Roe America - CPV  
Killer Hertz - DC  
KQL Kung Fu: Finding the Needle in the Haystack in Your Azure Environments - CLV  
Last chance to pick up drives at the DDV - DDV  
Latest and Greatest in Incident Response - BTV  
LATMA - Lateral movement analyzer - AIV  
Lawyers Meet - SOC  
Leak The Planet: Veritatem cognoscere non pereat mundus - DC  
Lend me your IR's! - BTV  
Less SmartScreen More Caffeine – ClickOnce (Ab)Use for Trusted Code Execution - DC  
Let's Dance in the Cache - Destabilizing Hash Table on Microsoft IIS - DC  
Literal Self-Pwning: Why Patients - and Their Advocates - Should Be Encouraged to Hack, Improve, and Mod Med Tech - DC  
Low Code High Risk: Enterprise Domination via Low Code Abuse - DC  
LSASS Shtinkering: Abusing Windows Error Reporting to Dump LSASS - DC  
Machine Learning Security Evasion Competition Launch - AIV  
Making the most of Microsoft cloud bug bounty programs: How I made in \$65,000 USD in bounties in 2021 - CLV  
Making Your SOC Suck Less - BTV  
Malicious memory techniques on Windows and how to spot them - BTV  
Malware Hunting - Discovering techniques in PDF malicious - BTV  
Mass Disinformation Operations - How to detect and assess Ops with OSINT & SOCMINT tools and techniques - MIV  
Master Class: Delivering a New Construct in Advanced Volatile Memory Analysis for Fun and Profit - WS  
Medeco cam lock exploit "an old attack made new again" - LPV  
Medical Device Hacking: A hands on introduction - BHV  
Meet the Digital Lab at Consumer Reports - SOC  
Meet the EFF - SOC  
Meet the Feds: CISA Edition (Lounge) - PLV  
Meet the Feds: DHS Edition (Lounge) - PLV  
Memento Vivere: A connected light installation on cerebral (dys)function - BHV  
Memfini - A systemwide memory monitor interface for linux - DL  
Merch (formerly swag) Area Open -- README - DC  
Merch (formerly swag) Area Open -- README - DC  
Merch (formerly swag) Area Open -- README - DC

Mercury - DL  
Metal and Fire... Copying Keys via Mold and Cast Tactics - LPV  
Mitigating vulnerabilities in two-factor authentication in preventing account takeover - RHV  
Movie Night Double Feature - Arrival & Real Genius - SOC  
Movie Night Double Feature - The Conversation & The 13th Floor - SOC  
Movie-Style Hardware Hacking - HHV  
Moving Regulation Upstream - An Increasing focus on the Role of Digital Service Providers - PLV  
Multi-Stakeholder Online Harm Threat Analysis - MIV  
My First Hack Was in 1958 (Then A Career in Rock'n'Roll Taught Me About Security) - DC  
NASA + Healthcare ... - BHV  
Natural Disasters and International Supply Chains: Biomedical and Pharmaceutical Review - BHV  
Near and Far: Securing On and Off Planet Networks at JPL - ASV  
Network Hacking 101 - WS  
Neurodiversity in Cybersecurity: Find Your Competitive Advantage! - BICV  
Night of the Ninjas - Entertainment - SOC  
No bricks without clay - Data Fusion and Duplication in Cybersecurity - DDV  
No-Code Malware: Windows 11 At Your Service - DC  
Not Feeling Yourself: User Spoofing and Other Disinformation Exploits - MIV  
OAuth-some Security Tricks: Yet more OAuth abuse - CLV  
Obsidian CTH Live: Killchain 1 Walkthrough - BTV  
Obsidian CTH Live: Killchain 3 Walkthrough - BTV  
Obsidian CTH: Go Phish: Visualizing Basic Malice - BTV  
Obsidian CTH: Hunting for Adversary's Schedule - BTV  
Obsidian CTH: Sniffing Compromise: Hunting for Bloodhound - BTV  
Obsidian CTH: The Logs are Gone? - BTV  
Obsidian CTI: Generating Threat Intelligence from an Incident - BTV  
Obsidian CTI: Operationalizing Threat Intelligence - BTV  
Obsidian Forensics: Creating a custom Velociraptor collector - BTV  
Obsidian Forensics: Kill Chain 1 Endpoint Forensics Walkthrough - BTV  
Obsidian Forensics: Kill Chain 3 Endpoint Forensics Walkthrough - BTV  
Obsidian Forensics: KillChain1 - Adventures in Splunk and Security Onion - BTV  
Obsidian Forensics: KillChain3 - Continued Adventures in Splunk and Security Onion - BTV  
Obsidian Forensics: The Importance of Sysmon for Investigations - BTV  
Obsidian Forensics: Using Chainsaw to Identify Malicious Activity - BTV  
Obsidian Live: Eating the Elephant 1 byte at a Time - BTV  
Obsidian Live: May We Have the OODA Loops? - BTV  
Obsidian REM: Long Walks On The Beach: Analyzing Collected PowerShells - BTV  
Obsidian REM: Phishing In The Morning: An Abundance of Samples! - BTV  
Obsidian: IR - Final Reporting Made Exciting\* - BTV  
Obsidian: IR - It all starts here, scoping the incident - BTV  
Obsidian: IR - Mise En Place for Investigations - BTV  
Obsidian: IR - OODA! An hour in incident responder life - BTV  
Off the grid - Supplying your own power - HRV  
Offensive Cyber Industry Roundtable - PLV  
Offensive IoT Exploitation - PT  
Offensive IoT Exploitation - PT  
Old Malware, New tools: Ghidra and Commodore 64, why understanding old malicious software still matters - DC  
Oli: A Simpler Pi-Star Replacement - HRV  
Once More Unto the Breach: Federal Regulators' Response to Privacy Breaches and Consumer Harms - CPV  
One Bootloader to Load Them All - DC  
OopsSec -The bad, the worst and the ugly of APT's operations security - DC  
OPAQUE is Not Magic - CPV  
OpenCola. The AntiSocial Network - DC  
Opening Remarks on the State of AI & Security - AIV  
OpenTDF - DL

Out of the Abyss: Surviving Vulnerability Management - BHV

Owned or pwned? No peakin' or tweakin'! - CPV

Packet Sender - DL

Panel - "So It's your first DEF CON" - How to get the most out of DEF CON, What NOT to do. - DC

Panel - DEF CON Policy Dept - What is it, and what are we trying to do for hackers in the policy world? - DC

Panel: Ask-a-ham - HRV

PCILeech and MemProcFS - DL

Pen Test Partner Power Hour - ASV

Pen Test Partners A320 Simulator - ASV

Pentesting Industrial Control Systems 101: Capture the Flag! - WS

Perimeter Breached! Hacking an Access Control System - DC

Phreaking 2.0 - Abusing Microsoft Teams Direct Routing - DC

PII: The Privacy Zombie - CPV

Pilots and Hackers Meetup - SOC

Pivoting, Tunneling, and Redirection Master Class - WS

Please deposit 30c: A history of payphone locks that lead to one of the most secure locks ever made. - LPV

PMR - PT & VA Management & Reporting - DL

Positive Identification of Least Significant Bit Image Steganography - CPV

Practical Dark Web Hunting using Automated Scripts - BTV

Practical Secure Code Review - PT

Practical Secure Code Review - PT

Pragmatic API Exploration - PT

Pragmatic API Exploration - PT

PreAuth RCE Chains on an MDM: KACE SMA - DC

Prizes announced for HHV Rube Goldberg Machine, Make Your Own Use Contest, and Bring the Other Half - HHV

Process injection: breaking all macOS security layers with a single vulnerability - DC

Project Obsidian: Panel Discussion - BTV

Protect Our Pентest Tools! Perks and Hurdles in Distributing Red Team Tools - PLV

Protect/hunt/respond with Fleet and osquery - WS

Prowler Open Source Cloud Security: A Deep Dive Workshop - CLV

PSA: Doorbell Cameras Have Mics, Too - CPV

Pulling Passwords out of Configuration Manager: Practical Attacks against Microsoft's Endpoint Management Software - DC

Purple Teaming & Adversary Emulation in the Cloud with Stratus Red Team - CLV

Pursuing Phone Privacy Protection [WORKSHOP] - CPV

Quantum Snake Oil? What Ailments Can It Cure? - ASV

Queercon Mixer - SOC

Queercon Mixer - SOC

Queercon Mixer - SOC

Queercon Party - SOC

Radical inclusivity and intersectionality in the biohacking world - BHV

Ransomware ATT&CK and Defense - BTV

Red Balloon Failsat Challenges - ASV

Red Balloon Failsat Challenges - ASV

Red Balloon Failsat Challenges - ASV

Reflections on 9 Years of CPV - CPV

ResidueFree - DL

Resumé Review and Career Guidance Session - ASV

Resumé Review and Career Guidance Session - ASV

Return-Oriented Policy Making for Open Source and Software Security - PLV

Reversing An M32C Firmware – Lesson Learned From Playing With An Uncommon Architecture - HHV

Reversing the Original Xbox Live Protocols - DC

RingHopper – Hopping from User-space to God Mode - DC

RoboSumo - HHV

Rock the Cash Box - RHV

Running Rootkits Like A Nation-State Hacker - DC

Safecracking for Everyone - LPV

Satellite Eavesdropping with DDS - ASV

Satellite Eavesdropping with DDS - ASV

Satellite Eavesdropping with DDS - ASV

Save The Environment (Variable): Hijacking Legitimate Applications with a Minimal Footprint - DC

Scaling the Security Researcher to Eliminate OSS Vulnerabilities Once and For All - DC

Secure by Design - Facilities design cybersecurity - BHV

Securing and Standardizing Data Rights Requests with a Data Rights Protocol - CPV

Securing Industrial Control Systems from the core: PLC secure coding practices - WS

Securing Smart Contracts - WS

Securing the Future of Aviation CyberSecurity - ASV

Securing Web Apps - WS

Security at Every Step: The TL;DR on Securing Your AWS Code Pipeline - CLV

Security Misconfigurations in the Cloud - "Oh Look, something fluffy, poke, poke, poke" - CLV

Self No-Fly Area Designing for UAV - ASV

SharpSCCM - DL

Shopping for Vulnerabilities - How Cloud Service Provider Marketplaces can Help White and Black Hat Vulnerability

Research - CLV

Sign of the Times: Exploiting Poor Validation of AWS SNS SigningCertUrl - CLV

SimPPL: Simulating Social Networks and Disinformation - MIV

So long, PBKDF2! The end of password-based key derivation - PWV

Solana JIT: Lessons from fuzzing a smart-contract compiler - DC

Space Jam: Exploring Radio Frequency Attacks in Outer Space - DC

Space ISAC: Protecting Our Space Assets - ASV

SquarePhish - Phishing Office 365 using QR Codes and Oauth 2.0 Device Code Flow - CLV

State of the Model - BICV

STrace - A DTrace on windows reimplementations. - DC

Surviving and Designing for Survivors - CPV

svachal + machinescli - DL

Take Your Security Skills From Good to Better to Best! - BTV

Taking a Dump In The Cloud - DC

Taking Down the Grid - SKY

TBA - DC

TCP/IP Deep Dive for Ethical Hackers – Featuring Wireshark - PT

TCP/IP Deep Dive for Ethical Hackers – Featuring Wireshark - PT

Tear Down this Zywall: Breaking Open Zyxel Encrypted Firmware - DC

That's No Moon -- A Look at the Space Threat Environment - ASV

The "Why" of Lock Picking - LPV

The Art of Modern Malware Analysis: Initial Infection Malware, Infrastructure, and C2 Frameworks - WS

The Big Rick: How I Rickrolled My High School District and Got Away With It - DC

The Call is Coming From Inside The Cluster: Mistakes that Lead to Whole Cluster Pwnership - DC

The Chaos of Coding with Language Models - AIV

The COW (Container On Windows) Who Escaped the Silo - DC

The CSRF Resurrections! Starring the Unholy Trinity: Service Worker of PWA, SameSite of HTTP Cookie, and Fetch - DC

The Dark Tangent & Mkfactor - Welcome to DEF CON & The Making of the DEF CON Badge - DC

The deadly state of surveillance capitalism in healthcare - CPV

The DFIR Report Homecoming Parade Panel - BTV

The Emerging Space - Cyber Warfare Theatre - ASV

The Evil PLC Attack: Weaponizing PLCs - DC

The GACWR Story: Building a Black Owned Cyber Range - BICV

The hitchhacker's guide to iPhone Lightning & JTAG hacking - DC

The hybrid strategies of autocratic states: narrative characteristics of disinformation campaigns in relation to issues of a scientific-health nature - MIV

The Journey From an Isolated Container to Cluster Admin in Service Fabric - DC

The Last Log4Shell Talk You Need - BICV

The least secure biometric lock on Earth? - LPV

The Multiverse of Madness: Navigating the 50-State Approach to Privacy and Security - CPV

The PACMAN Attack: Breaking PAC on the Apple M1 with Hardware Attacks - DC

The Purple Malware Development Approach - WS

The Richest Phisherman in Colombia - SKY

The Right Way To Do Wrong: Physical security secrets of criminals and professionals alike - LPV

The Use of AI/ML in Offensive Security Operations - AIV

TheAllCommander - DL

This one time, at this Hospital, I got Ransomware - SKY

Threat Hunt Trilogy: A Beast in the Shadow! - BTV

Threat hunting? Ain't nobody got time for that... - BICV

Thursday Opening Party - Entertainment - SOC

Tools for Fighting Disinformation - MIV

Tor: Darknet Opsec By a Veteran Darknet Vendor & the Hackers Mentality - DC

Toto, I've a feeling we're not on a VPN anymore - CPV

Toxic BBQ - SOC

Trace me if you can: Bypassing Linux Syscall Tracing - DC

Tracking Military Ghost Helicopters over our Nation's Capital - DC

Tracking Scams and Disinformation by Hacking Link Shorteners - MIV

Trailer Shouting: Talking PLC4TRUCKS Remotely with an SDR - DC

UFOs, Alien Life, and the Least Untruthful Things I Can Say. - DC

unblob - towards efficient firmware extraction - DL

Uncovering multi-platform misinformation campaigns with Information Tracer - MIV

Understanding, Abusing and Monitoring AWS AppStream 2.0 - CLV

us-east-1 Shuffle: Lateral Movement and other Creative Steps Attackers Take in AWS Cloud Environments and how to detect them - CLV

Uwb Security Primer: Rise Of A Dusty Protocol - HHV

Vajra - Your Weapon To Cloud - DL

VETCON - SOC

Village Areas Open (Generally) - DC

Village Areas Open (Generally) - DC

Village Areas Open (Generally) - DC

Voldrakus: Using Consent String Steganography to Exfiltrate Browser Fingerprinting Data - CPV

Voter Targeting, Location Data, and You - SKY

Vulnerability Assessment of a Satellite Simulator - ASV

Wakanda Land - DL

Weaponizing Windows Syscalls as Modern, 32-bit Shellcode - DC

Weather Proofing GCP Defaults - CLV

Web Monetization: A privacy-preserving and open way to earn from Content - MIV

Web Shell Hunting - BTV

What your stolen identity did on its CoViD vacation - SKY

When The "IT" Hits The Fan, Stick To the Plan - BICV

Where there's a kiosk, there's an escape - BHV

Who Contains the "Serverless" Containers? - CLV

Whose Slide Is It Anyway? (WSIIA) - SOC

Why did you lose the last PS5 restock to a bot Top-performing app-hackers business modules, architecture, and techniques - DC

Windows Defence Evasion and Fortification Primitives - WS

Wireless Keystroke Injection (WKI) via Bluetooth Low Energy (BLE) - DC

Xavier Memory Analysis Framework - DL

XR Technology Has 99 Problems and Privacy is Several of Them (PRE-RECORDED) - CPV

YARA Rules to Rule them All - BTV

You Have One New Appwntment - Hacking Proprietary iCalendar Properties - DC

You're <strike>Muted</strike>Rooted - DC

Your Amateur Radio License and You - HRV

Zero 2 Emulated Criminal: Intro to Windows Malware Dev - PT

Zero 2 Emulated Criminal: Intro to Windows Malware Dev - PT

Zuthaka: A Command & Controls (C2s) integration framework - DL

---

## Village Talk List

---

### AIV - Artificial Intelligence Village

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

Sched Page: <https://aivillage.org/defcon30/>

DC Discord Chan: <https://discord.com/channels/708208267699945503/732733090568339536>

---

PDT Times	Title	speaker
Friday		
09:30 - 10:50	Automate Detection with Machine Learning	Gavin Klondike
09:00 - 09:25	Opening Remarks on the State of AI & Security	Brian Pendleton,Sven Catt . . .
11:00 - 11:50	I'm not Keylogging you! Just some benign data co . . .	Harini Kannan
12:00 - 12:50	AI Village Keynote	Keith E. Sonderling
13:00 - 13:50	Machine Learning Security Evasion Competition Laun . . .	Hyrum Anderson
14:00 - 14:50	The Chaos of Coding with Language Models	Nick Dorion
15:00 - 15:50	LATMA - Lateral movement analyzer	Gal Sadeh
16:00 - 16:50	Panel: AI and Hiring Tech	
Saturday		
10:00 - 10:50	A few useful things to know about AI Red Teams	Sudipto Rakshit
11:00 - 11:50	Hands-on Hacking of Reinforcement Learning Systems	Dr. Amanda Minnich
12:00 - 12:50	A System for Alert Prioritization	Ben Gelman ,Salma Taoufi . . .
13:00 - 13:50	CatPhish Automation - The Emerging Use of Artifici . . .	Justin Hutchens
14:00 - 14:50	The Use of AI/ML in Offensive Security Operations	
15:00 - 15:50	Generative Art Tutorial	
16:00 - 17:30	AI Music Tutorial and Show	dadabots
Sunday		
09:00 - 10:20	Automate Detection with Machine Learning	Gavin Klondike
10:30 - 11:20	Attacks on Tiny Intelligence	Yuvaraj Govindarajulu
11:30 - 12:20	AI Trojan Attacks, Defenses, and the TrojAI Compet . . .	Taylor Kulp-Mcdowall
12:30 - 13:20	AI Village CTF Results and Q&A	Will Pearce
14:00 - 14:59	AI Village Closing Remarks	Sven Cattell,Brian Pendle . . .

## ASV - Aerospace Village

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

Sched Page: <https://aerospacevillage.org/events/upcoming-events/def-con-30/def-con-30-schedule/>

DC Discord Chan: <https://discord.com/channels/708208267699945503/732393044363444264>

PDT Times	Title	speaker
Friday		
09:00 - 16:59	California CyberSecurity Institute Space Grand Cha . . .	
10:00 - 16:59	Hack the Airport with Intelligenesis	
10:00 - 16:59	Hack the Airfield with DDS	
10:00 - 16:59	Satellite Eavesdropping with DDS	
10:00 - 15:59	Red Balloon Failsat Challenges	
10:00 - 11:59	Pen Test Partners A320 Simulator	
10:00 - 16:59	Hack-A-Sat Digital Twin Workshop	
10:00 - 10:50	Hack-A-Sat Team	
10:00 - 16:59	Amazon Web Services Aerospace and Satellite Jam	
10:00 - 15:59	Boeing ARINC 429 Airplane Challenge and CTF	
11:30 - 11:55	DDS Space Signal Lab	James Pavur
11:00 - 11:25	That's No Moon -- A Look at the Space Threat Envir . . .	Mike Campanelli
12:00 - 12:50	Hackers Help Make My Airline Secure	Deneen Defiore
12:00 - 16:59	Hack-A-Sat Aerospace PiSat Challenge	
13:00 - 14:59	Resumé Review and Career Guidance Session	
13:00 - 13:25	Cyber Star Card Game Tutorial	Rick White
13:00 - 12:59	Cyber Star® Competition Presented by The Space IS . . .	
13:00 - 14:59	Pen Test Partners A320 Simulator	
13:30 - 13:55	Securing the Future of Aviation CyberSecurity	Timothy Weston
14:00 - 14:50	Final Boarding Call for Cyber Policy Airlines Flig . . .	Rebecca Ash,Ayan Islam,Ma . . .
15:00 - 15:50	Ask an Airport CISO	Aakinn Patel
16:00 - 16:50	Pen Test Partner Power Hour	Ken Munro,Alex Lomas
Saturday		
10:00 - 16:59	Hack the Airport with Intelligenesis	
10:00 - 16:59	Hack the Airfield with DDS	
10:00 - 10:25	Building Your Own Satellite Ground Station	Eric Escobar
10:30 - 10:55	Quantum Snake Oil? What Ailments Can It Cure?	Jose Pizarro
10:00 - 16:59	Satellite Eavesdropping with DDS	
10:00 - 15:59	Red Balloon Failsat Challenges	
10:00 - 11:59	Pen Test Partners A320 Simulator	

PDT Times	Title	speaker
10:00 - 16:59	Hack-A-Sat Digital Twin Workshop	
10:00 - 16:59	Amazon Web Services Aerospace and Satellite Jam	
10:00 - 15:59	Boeing ARINC 429 Airplane Challenge and CTF	
11:00 - 11:50	Cyber Threats Against Aviation Systems: The Only T . . .	Teresa Merklin
12:00 - 16:59	Hack-A-Sat Aerospace PiSat Challenge	
12:00 - 12:50	Introduction to Aircraft Networks and Security Des . . .	Sean Sullivan
13:00 - 14:59	Resumé Review and Career Guidance Session	
13:00 - 14:59	Pen Test Partners A320 Simulator	
13:00 - 13:50	Hunting for Spacecraft Zero Days Using Digital Twi . . .	Brandon Bailey
14:30 - 14:55	The Emerging Space - Cyber Warfare Theatre	Eytan Tepper
14:00 - 14:25	Vulnerability Assessment of a Satellite Simulator	Henry Haswell
15:00 - 15:50	Near and Far: Securing On and Off Planet Networks . . .	Wes Gavins
16:00 - 16:50	Space ISAC: Protecting Our Space Assets	
Sunday		
10:00 - 12:59	Hack the Airport with Intelligenesis	
10:00 - 12:59	Hack the Airfield with DDS	
10:00 - 12:59	Satellite Eavesdropping with DDS	
10:00 - 10:25	Self No-Fly Area Designing for UAV	Utku Yildirim
10:00 - 11:59	Red Balloon Failsat Challenges	
10:30 - 11:20	Control Acquisition Attack of Aerospace Systems by . . .	Garrett Jares
10:00 - 12:59	Hack-A-Sat Digital Twin Workshop	
10:00 - 11:59	Pen Test Partners A320 Simulator	
11:30 - 11:55	Formalizing Security Assessment for Uncrewed Aeria . . .	Rudy Mendoza, Ronald Brobe . . .
12:00 - 12:50	Drones and Civil Liberties	Andrés Arrieta

[Return to Index](#)

## BHV - Bio Hacking Village

Hours: Fri: 10:00 - 18:00 - Sat: 10:00 - 18:00 - Sun: 10:00 - 13:00

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

Sched Page: <https://www.villageb.io/2022bhvspeakers>

DC Discord Chan: <https://discord.com/channels/708208267699945503/735273390528528415>

PDT Times	Title	speaker
Friday		
10:00 - 10:30	BioHacking Village Keynote	Nina Alli
10:30 - 10:59	A Capitalist approach to hospital security	Eirick Luraas
11:30 - 11:59	Department of Defense 5G Telemedicine and Medical . . .	Paul Young
11:00 - 11:59	Where there's a kiosk, there's an escape	Michael Aguilar (v3ga)

PDT Times	Title	speaker
12:00 - 12:30	Gird your loins: premise and perils of biomanufacturing	Nathan Case
12:30 - 13:30	How to stop Surveillance Capitalism in Healthcare	Andrea Downing,Jillian Sizemore
13:30 - 13:59	DIY Medicine With Unusual Uses for Existing FDA-Approved Drugs	Mixael S. Laufer
14:30 - 15:59	DIY MQTT IoT (or how you can turn your home into a smart house)	Cody Wayne Burkhart
16:30 - 17:59	Medical Device Hacking: A hands on introduction	Malcolm Galland
Saturday		
10:00 - 10:30	NASA + Healthcare ...	Dr. Josef Schmid
10:30 - 10:59	Faking Positive COVID Tests	Ken Gannon
11:00 - 11:59	How to Leverage MDS2 Data for Medical Device Security	Jeremy Linden
11:30 - 11:59	All information should be free (except the brain data)	Isabel Straw
12:00 - 12:30	Breaking the Intelligence Cycle - how to tailor in ...	Ohad Zaidenberg
13:00 - 13:30	Out of the Abyss: Surviving Vulnerability Management	Leo Nendza, Mike Kijewski
13:30 - 14:30	Radical inclusivity and intersectionality in the b ...	Berkelly Gonzalez
14:30 - 14:59	Natural Disasters and International Supply Chains: ...	Jorge Acevedo Canabal
15:00 - 15:30	Secure by Design - Facilities design cybersecurity	David Brearley
16:00 - 16:30	Call for Evidence: Informing the Biological Security	Mariam Elgabry
16:30 - 17:59	How to Build DIY Lifesaving Medical Devices	Four Thieves Vinegar Collective
Sunday		
10:30 - 11:59	Memento Vivere: A connected light installation on ...	Rick Martinez Herrera
12:30 - 13:59	In the eye of the Beholder	

[Return to Index](#)

## BICV - Blacks in Cybersecurity

Home Page: <https://www.blacksin cyberconf.com/bic-village>  
Sched Page: <https://www.blacksin cyberconf.com/bic-village>

PDT Times	Title	speaker
Friday		
10:00 - 10:30	The GACWR Story: Building a Black Owned Cyber Range	Jovonni Pharr,GACWR Team
11:00 - 11:59	Creating More Black Hackers: Growth Systems for Cybersecurity	Segun Ebenezer Olaniyan
12:00 - 12:30	"The Man" in the Middle	Alexis Hancock
14:00 - 14:30	DEI in Cybersecurity (Breaking through the barrier)	Damian Grant
16:00 - 16:59	The Last Log4Shell Talk You Need	Ochuan Marshall
Saturday		
10:00 - 10:45	When The "IT" Hits The Fan, Stick To the Plan	Levone Campbell
11:00 - 11:45	Cryptocurrency: A Bridge Across the Digital Divide	Stephanie Barnes
12:00 - 12:30	Decolonizing Cybersecurity	Birhanu Eshete

PDT Times	Title	speaker
13:00 - 13:59	State of the Model	Jovonni Pharr,GACWR Team
15:00 - 15:30	Threat hunting? Ain't nobody got time for that....	Nick Gobern
16:00 - 16:30	Neurodiversity in Cybersecurity: Find Your Competi ...	Kassandra Pierre,Nathan C ...

[Return to Index](#)

## BTV - Blue Team Village

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

Sched Page: <https://dc30.blueteamvillage.org/call-for-content-2022/schedule/#>

DC Discord Chan: <https://discord.com/channels/708208267699945503/732454317658734613>

PDT Times	Title	speaker
Friday		
10:00 - 10:30	Blue Team Village Opening Ceremony	
10:30 - 11:30	Obsidian Live: Eating the Elephant 1 byte at a Tim ...	aviditas,ChocolateCoat
10:30 - 11:30	Obsidian Forensics: Kill Chain 1 Endpoint Forensic ...	Omenscan
10:30 - 11:30	Obsidian CTH: Go Phish: Visualizing Basic Malice	SamunoskeX
11:30 - 12:30	Obsidian: IR - It all starts here, scoping the inc ...	ChocolateCoat
11:30 - 12:30	Obsidian CTI: Generating Threat Intelligence from ...	Stephanie G.,l00sid,tthev ...
11:45 - 12:45	Malicious memory techniques on Windows and how to ...	Connor Morley
11:00 - 11:30	Attribution and Bias: My terrible mistakes in thre ...	Seongsu Park
11:00 - 12:30	Practical Dark Web Hunting using Automated Scripts	Apurv Singh Gautam
13:00 - 13:59	Obsidian Forensics: KillChain1 - Adventures in Spl ...	ExtremePaperClip,Omenscan ...
13:00 - 13:59	Obsidian: IR - Mise En Place for Investigations	aviditas,ChocolateCoat,Co ...
13:00 - 13:59	Obsidian CTH: Hunting for Adversary's Schedule	Cyb3rHawk
13:00 - 13:59	Improving security posture of MacOS and Linux with ...	Michael Epping,Mark Morow ...
13:00 - 14:30	Ransomware ATT&CK and Defense	Ronny Thammasathiti,Danie ...
14:00 - 14:59	Obsidian CTH Live: Killchain 1 Walkthrough	
14:00 - 14:59	Obsidian Forensics: The Importance of Sysmon for I ...	ExtremePaperClip
14:00 - 14:59	Obsidian REM: Long Walks On The Beach: Analyzing C ...	Alison N
14:15 - 15:15	Lend me your IR's!	Matt Scheurer
15:00 - 15:59	Heavyweights: Threat Hunting at Scale	Sherrod DeGrippo,Ashlee B ...
15:30 - 16:30	Malware Hunting - Discovering techniques in PDF ma ...	Filipi Pires
16:00 - 16:59	Take Your Security Skills From Good to Better to B ...	Ricky Banda,Neumann Lim ( ...
16:45 - 16:59	YARA Rules to Rule them All	Saurabh Chaudhary
17:00 - 17:59	Blue Teaming Cloud: Security Engineering for Cloud ...	KyleHaxWhy,Cassandra Youn ...
Saturday		
10:30 - 11:30	Obsidian Forensics: KillChain3 - Continued Adventu ...	Omenscan,Wes Lambert,Extr ...
10:30 - 11:30	Obsidian: IR - OODA! An hour in incident responder ...	juju43

PDT Times	Title	speaker
10:30 - 11:30	Obsidian CTH: Sniffing Compromise: Hunting for Blo . . .	CerealKiller
11:30 - 12:30	Obsidian Forensics: Kill Chain 3 Endpoint Forensic . . .	Omenscan
11:30 - 12:30	Obsidian CTI: Operationalizing Threat Intelligence	Stephanie G.,l00sid,tthev . . .
11:00 - 11:59	Threat Hunt Trilogy: A Beast in the Shadow!	Dr. Meisam Eslahi
11:00 - 14:59	Web Shell Hunting	Joe Schottman
12:15 - 12:45	Even my Dad is a Threat Modeler!	Sarthak Taneja
13:00 - 13:59	Obsidian CTH Live: Killchain 3 Walkthrough	aviditas,CountZ3r0
13:00 - 13:59	Obsidian: IR - Final Reporting Made Exciting*	Alison N
13:00 - 13:59	Obsidian REM: Phishing In The Morning: An Abundanc . . .	Kostas,ICSNick - Nicklas . . .
13:00 - 13:59	The DFIR Report Homecoming Parade Panel	CountZ3r0,juju43
14:00 - 14:59	Obsidian Live: May We Have the OODA Loops?	Wes Lambert,Omenscan
14:30 - 14:59	Obsidian Forensics: Creating a custom Velociraptor . . .	Danny D. Henderson Jr (B4 . . .
14:00 - 14:59	Obsidian Forensics: Using Chainsaw to Identify Mal . . .	ExtremePaperClip
14:00 - 14:59	Obsidian CTH: The Logs are Gone?	Anton Ovrutsky
14:15 - 14:45	Hunting Malicious Office Macros	AJ King,Jake Williams,Kri . . .
15:00 - 15:59	Challenges in Control Validation	Gilmar Esteves
15:00 - 15:15	Horusec - Brazilian SAST help World	Shawn Thomas,Carson Zimme . . .
16:00 - 16:59	Making Your SOC Suck Less	Lauren Proehl,plug,LitMoo . . .
17:00 - 17:59	Latest and Greatest in Incident Response	
Sunday		
11:00 - 11:59	Backdoors & Breaches, Back to the Stone Age!	
12:00 - 12:59	Project Obsidian: Panel Discussion	
13:00 - 13:59	Blue Team Village Closing Ceremony	

[Return to Index](#)

## CLV - Cloud Village

Home Page: <https://cloud-village.org/>  
 Sched Page: <https://cloud-village.org/#talks>  
 DC Discord Chan: <https://discord.com/channels/708208267699945503/732733373172285520>

PDT Times	Title	speaker
Friday		
10:10 - 10:50	Automating Insecurity in Azure	Karl Fosaaen
10:00 - 10:10	Cloud Village Opening Note	Jayesh Singh Chauhan
10:50 - 11:30	Making the most of Microsoft cloud bug bounty prog . . .	Nestori Syynimaa
11:30 - 12:10	Flying Under Cloud Cover: Built-in Blind Spots in . . .	Noam Dahan
12:30 - 13:10	Weather Proofing GCP Defaults	Shannon McHale
12:10 - 12:30	A ransomware actor looks at the clouds: attacking . . .	Jay Chen

PDT Times	Title	speaker
13:40 - 14:20	Sponsored Talk	
13:10 - 13:40	Security at Every Step: The TL;DR on Securing Your ...	Cassandra Young (muteki)
14:20 - 14:50	Shopping for Vulnerabilities - How Cloud Service P...	Alexandre Sieira
15:00 - 16:59	Prowler Open Source Cloud Security: A Deep Dive Wo...	Toni de la Fuente
Saturday		
10:00 - 10:40	OAuth-some Security Tricks: Yet more OAuth abuse	Jenko Hwong
10:40 - 11:20	Who Contains the “Serverless” Containers?	Daniel Prizmant
11:20 - 11:59	Purple Teaming & Adversary Emulation in the Cloud ...	Christophe Tafani-Derepee ...
12:00 - 12:30	SquarePhish - Phishing Office 365 using QR Codes a ...	Kamron Talebzadeh,Nevada ...
12:30 - 13:10	Security Misconfigurations in the Cloud - "Oh Look ...	Kat Fitzgerald
13:10 - 13:40	BrokenbyDesign: Azure   Get started with hacking A ...	Siebren Kraak,Roy Stultie ...
13:40 - 14:20	us-east-1 Shuffle: Lateral Movement and other Crea ...	Felipe Espósito
14:20 - 14:50	Access Undenied on AWS - Troubleshooting AWS IAM A ...	Noam Dahan
15:00 - 16:59	KQL Kung Fu: Finding the Needle in the Haystack in ...	Darwin Salazar
Sunday		
10:00 - 10:40	Understanding, Abusing and Monitoring AWS AppStrea ...	Rodrigo Montoro
10:40 - 11:20	How to do Cloud Security assessments like a pro in ...	Ricardo Sanchez
11:20 - 11:50	Cloud Sandboxes for Security Research - Fire from ...	Louis Barrett
11:50 - 12:30	Deescalate the overly-permissive IAM	Jay Chen
12:30 - 12:50	Sign of the Times: Exploiting Poor Validation of A ...	Eugene Lim
12:50 - 13:30	Cloud Defaults are Easy Not Secure	Igal Flegmann
13:30 - 13:45	Cloud Village Closing Note	Jayesh Singh Chauhan

[Return to Index](#)

## CPV - Crypto Privacy Village

Home Page: <https://cryptovillage.org/>  
 Sched Page: <https://cryptovillage.org/>  
 DC Discord Chan: <https://discord.com/channels/708208267699945503/732734002011832320>

PDT Times	Title	speaker
Friday		
10:30 - 10:59	Back to School! Hello RSA... and beyond!	Mike Guirao
11:30 - 11:59	OPAQUE is Not Magic	Steve Thomas
11:00 - 11:30	Positive Identification of Least Significant Bit I ...	Michael Pelosi
12:00 - 12:30	PSA: Doorbell Cameras Have Mics, Too	Yael Grauer,Matthew Guari ...
13:30 - 13:59	How to Respond to Data Subject Access Requests	Irene Mo
13:00 - 13:30	Reflections on 9 Years of CPV	Whitney Merrill
14:30 - 14:59	The Multiverse of Madness: Navigating the 50-State ...	Anthony Hendricks

PDT Times	Title	speaker
14:00 - 14:30	Securing and Standardizing Data Rights Requests wi . . .	Ginny Fahs,Ryan Rix,Dazza . . .
15:00 - 15:30	ID theft insurance - The Emperor's new clothes?	Per Thorsheim
16:45 - 17:30	Owned or pwned? No peakin' or tweakin'!	Nick Vidal,Richard Zak
16:00 - 16:45	Once More Unto the Breach: Federal Regulators' Res . . .	Erie Meyer,Alexis Goldste . . .
17:30 - 17:59	[T]OTPs are not as secure as you might believe	Santiago Kantorowicz
Saturday		
10:30 - 10:59	Fun with Factoring Large Prime Numbers	p80n,r3c0d3
11:00 - 11:30	Introducing the Abusability Testing Framework (V1)	Nicole Chi,Ji Su Yoo,Avi . . .
11:30 - 12:30	Jailed By a Google Search Part 2: Abortion Surveil . . .	Kate Bertash
13:00 - 13:45	Cryptle: a secure multi-party Wordle clone with En . . .	Tom Dohrmann,Richard Zak, . . .
13:45 - 14:30	Exploring Unprecedented Avenues for Data Harvestin . . .	Gonzalo Munilla Garrido,V . . .
14:30 - 14:59	The deadly state of surveillance capitalism in hea . . .	Valencia Robinson,Mike Mi . . .
15:30 - 16:15	Capturing Chaos: Harvesting Environmental Entropy	Carey Parker
16:15 - 16:59	Toto, I've a feeling we're not on a VPN anymore . . .	Jonathan Tomek
17:00 - 17:59	Pursuing Phone Privacy Protection [WORKSHOP]	Mauricio Tavares,Matt Nas . . .
Sunday		
10:30 - 10:59	XR Technology Has 99 Problems and Privacy is Sever . . .	Suchi Pahi,Calli Schroede . . .
11:30 - 11:59	Finding Crypto: Inventorying Cryptographic Operati . . .	Kevin Lai
11:00 - 11:30	Voldrakus: Using Consent String Steganography to E . . .	Kaileigh McCrea
12:00 - 12:30	Surviving and Designing for Survivors	Avi Zajac
12:45 - 13:30	PII: The Privacy Zombie	Alisha Kloc
13:30 - 14:15	Cryptosploit	Matt Cheung,Benjamin Hend . . .
14:15 - 14:59	AES-GCM common pitfalls and how to work around the . . .	Santiago Kantorowicz

[Return to Index](#)

## DC - DEF CON Talks

Home Page: <https://defcon.org/html/defcon-30/dc-30-index.html>  
Sched Page: <https://defcon.org/html/defcon-30/dc-30-schedule.html>

PDT Times	Title	speaker
Thursday		
07:00 - 19:59	Human Registration Open	
Friday		
08:00 - 18:59	Human Registration Open	
09:00 - 15:59	Merch (formerly swag) Area Open -- README	
10:00 - 10:45	Old Malware, New tools: Ghidra and Commodore 64, w . . .	Cesare Pizzi
10:30 - 11:15	OopsSec -The bad, the worst and the ugly of APT' . . .	Tomer Bar

PDT Times	Title	speaker
10:00 - 10:20	Computer Hacks in the Russia-Ukraine War	Kenneth Geers
10:00 - 10:45	Panel - "So It's your first DEF CON" - How to get . . .	DEF CON Goons
10:00 - 11:15	Panel - DEF CON Policy Dept - What is it, and what . . .	DEF CON Policy Dept
10:00 - 17:59	Vendor Area Open	
10:00 - 17:59	Village Areas Open (Generally)	
11:00 - 11:45	The PACMAN Attack: Breaking PAC on the Apple M1 wi . . .	Joseph Ravichandran
11:30 - 11:50	Running Rootkits Like A Nation-State Hacker	Omri Misgav
11:00 - 11:45	The Dark Tangent & Mkfactor - Welcome to DEF CON . . .	The Dark Tangent,Michael . . .
11:30 - 12:15	DEF CON Policy Dept - Special Edition Policy Talk	DEF CON Policy Dept
12:00 - 12:45	Avoiding Memory Scanners: Customizing Malware to E . . .	Kyle Avery
12:00 - 12:45	One Bootloader to Load Them All	Jesse Michael,Mickey Shka . . .
12:00 - 12:45	Glitched on Earth by humans: A Black-Box Security . . .	Lennert Wouters
12:30 - 13:15	DEF CON Policy Dept - Special Edition Policy Talk	DEF CON Policy Dept
13:00 - 13:20	Backdooring Pickles: A decade only made things wor . . .	ColdwaterQ
13:30 - 13:50	Weaponizing Windows Syscalls as Modern, 32-bit She . . .	Tarek Abdelmotaleb,Dr. Br . . .
13:00 - 13:45	You're <strike>Muted</strike>Rooted	Patrick Wardle
13:00 - 13:45	Emoji Shellcoding: , , and	Georges-Axel Jaloyan,Hadr . . .
13:30 - 14:15	DEF CON Policy Dept - Special Edition Policy Talk	DEF CON Policy Dept
14:00 - 14:45	Process injection: breaking all macOS security lay . . .	Thijs Alkemade
14:30 - 15:15	Trace me if you can: Bypassing Linux Syscall Traci . . .	Rex Guo,Junyuan Zeng
14:00 - 14:20	Phreaking 2.0 - Abusing Microsoft Teams Direct Rou . . .	Moritz Abrell
14:00 - 14:45	Space Jam: Exploring Radio Frequency Attacks in Ou . . .	James Pavur
14:30 - 15:15	Leak The Planet: Veritatem cognoscere non pereat m . . .	Xan North,Emma Best
15:00 - 15:45	LSASS Shtinkering: Abusing Windows Error Reporting . . .	Asaf Gilboa,Ron Ben Yitzh . . .
15:30 - 16:15	Browser-Powered Desync Attacks: A New Frontier in . . .	James Kettle
15:00 - 15:45	Exploring the hidden attack surface of OEM IoT dev . . .	Octavio Galland,Octavio G . . .
15:30 - 16:15	How Russia is trying to block Tor	Roger Dingledine
16:00 - 16:45	Wireless Keystroke Injection (WKI) via Bluetooth L . . .	Fernando Perera,Jose Pico
16:30 - 17:15	A dead man's full-yet-responsible-disclosure sys . . .	Yolan Romailler
16:00 - 16:45	Hacking ISPs with Point-to-Pwn Protocol over Ether . . .	Gal Zror
16:30 - 17:15	DEF CON Policy Dept - Special Edition Policy Talk	DEF CON Policy Dept
17:00 - 17:45	Let's Dance in the Cache - Destabilizing Hash Tabl . . .	Orange Tsai
17:30 - 17:50	Deanonymization of TOR HTTP hidden services	Ionut Cernica
17:00 - 17:45	Hunting Bugs in The Tropics	Daniel Jensen
17:30 - 18:15	DEF CON Policy Dept - Special Edition Policy Talk	DEF CON Policy Dept
18:00 - 18:45	Pulling Passwords out of Configuration Manager: Pr . . .	Christopher Panayi
18:00 - 18:45	Tear Down this Zywall: Breaking Open Zyxel Encrypt . . .	Jay Lagorio
18:00 - 18:45	Killer Hertz	Chris Rock
18:30 - 18:50	Dragon Tails: Supply-side Security and Internation . . .	Stewart Scott,Trey Herr
Saturday		
09:00 - 18:59	Human Registration Open	
09:00 - 15:59	Merch (formerly swag) Area Open -- README	
10:00 - 10:45	Scaling the Security Researcher to Eliminate OSS V . . .	Jonathan Leitschuh

PDT Times	Title	speaker
10:00 - 10:45	Literal Self-Pwning: Why Patients - and Their Advo . . .	Christian "quaddi" Dameff . . .
10:00 - 11:15	Brazil Redux: Short Circuiting Tech-Enabled Dystop . . .	Paul Roberts,Corynne McSh . . .
10:00 - 17:59	Vendor Area Open	
10:00 - 17:59	Village Areas Open (Generally)	
11:00 - 11:45	No-Code Malware: Windows 11 At Your Service	Michael Bargury
11:00 - 11:45	How To Get MUMPS Thirty Years Later (or, Hacking T . . .	Zachary Minneker
11:30 - 12:15	Reversing the Original Xbox Live Protocols	Tristan Miller
11:00 - 11:45	My First Hack Was in 1958 (Then A Career in Rock. . .	Winn Schwartau
12:00 - 12:45	All Roads leads to GKE's Host : 4+ Ways to Escape	Billy Jheng,Muhammad ALif . . .
12:00 - 12:20	The Evil PLC Attack: Weaponizing PLCs	Sharon Brizinov
12:30 - 13:15	Analyzing PIPEDREAM: Challenges in testing an ICS . . .	Jimmy Wylie
12:30 - 12:50	The hitchhacker's guide to iPhone Lightning & JT . . .	stacksmashing
12:00 - 12:20	Tracking Military Ghost Helicopters over our Natio . . .	Andrew Logan
12:30 - 13:15	UFOs, Alien Life, and the Least Untruthful Things . . .	Richard Thieme
13:00 - 13:45	Exploring Ancient Ruins to Find Modern Bugs: Disco . . .	Ophir Harpaz,Ben Barnea
13:30 - 14:15	Do Not Trust the ASA, Trojans!	Jacob Baines
13:00 - 13:45	Chromebook Breakout: Escaping Jail, with your frie . . .	Jimi Allee
13:30 - 14:15	HACK THE HEMISPHERE! How we (legally) broadcasted . . .	Andrew Green,Karl Koscher
14:00 - 14:45	The COW (Container On Windows) Who Escaped the Sil . . .	Eran Segal
14:30 - 15:15	Doing the Impossible: How I Found Mainframe Buffer . . .	Jake Labelle
14:00 - 14:45	OpenCola. The AntiSocial Network	John Midgley
14:30 - 14:50	Digging into Xiaomi's TEE to get to Chinese mone . . .	Slava Makkaveev
15:00 - 15:45	You Have One New Appwntment - Hacking Proprietary . . .	Eugene Lim
15:30 - 16:15	Perimeter Breached! Hacking an Access Control Syst . . .	Sam Quinn,Steve Povolny
15:30 - 15:50	Automotive Ethernet Fuzzing: From purchasing ECU t . . .	Woongjo choi,Soohwan Oh,J . . .
15:00 - 15:20	Déjà Vu: Uncovering Stolen Algorithms in Commerc . . .	Patrick Wardle,Tom McGuir . . .
15:00 - 15:20	The Big Rick: How I Rickrolled My High School Dist . . .	Minh Duong
15:30 - 16:15	Tor: Darknet Opsec By a Veteran Darknet Vendor & t . . .	Sam Bent
16:00 - 16:45	Low Code High Risk: Enterprise Domination via Low . . .	Michael Bargury
16:30 - 17:15	Defeating Moving Elements in High Security Keys	Bill Graydon
16:00 - 16:45	Trailer Shouting: Talking PLC4TRUCKS Remotely with . . .	Ben Gardiner,Chris Poore
16:30 - 17:15	Why did you lose the last PS5 restock to a bot Top . . .	Arik
17:00 - 17:45	Internal Server Error: Exploiting Inter-Process Co . . .	Martin Doyhenard
17:30 - 18:15	Black-Box Assessment of Smart Cards	Daniel Crowley
17:00 - 17:45	Hacking The Farm: Breaking Badly Into Agricultural . . .	Sick Codes
17:30 - 18:15	Crossing the KASM -- a webapp pentest story	Justin Gardner,Samuel Erb
18:00 - 18:45	The CSRF Resurrections! Starring the Unholy Trinit . . .	Dongsung Kim
18:30 - 18:50	Digital Skeleton Keys - We've got a bone to pick . . .	Miana E Windall,Micsen
Sunday		
09:00 - 14:59	Merch (formerly swag) Area Open -- README	
10:00 - 15:59	Human Registration Open	
10:00 - 15:59	Vendor Area Open	
10:00 - 14:59	Village Areas Open (Generally)	

PDT Times	Title	speaker
11:00 - 11:45	Save The Environment (Variable): Hijacking Legitim . . .	Wietze Beukema
11:00 - 11:45	STrace - A DTrace on windows reimplementa . . .	Stephen Eckels
11:00 - 11:45	Exploitation in the era of formal verification: a . . .	Adam Zabrocki,Alex Teresh . . .
11:00 - 11:45	emulation-driven reverse-engineering for finding v . . .	atlas
12:00 - 12:45	PreAuth RCE Chains on an MDM: KACE SMA	Jeffrey Hofmann
12:00 - 12:45	Defaults - the faults. Bypassing android permissio . . .	Nikita Kurtin
12:00 - 12:45	The Call is Coming From Inside The Cluster: Mistak . . .	Will Kline,Dagan Henderso . . .
12:00 - 12:45	Taking a Dump In The Cloud	Flangvik,Melvin Langvik
13:00 - 13:45	ElectroVolt: Pwning popular desktop apps while unc . . .	Max Garrett,Aaditya Puran . . .
13:00 - 13:45	The Journey From an Isolated Container to Cluster . . .	Aviv Sasson
13:00 - 13:45	Less SmartScreen More Caffeine – ClickOnce (Ab)U . . .	Nick Powers,Steven Flores
13:00 - 13:45	TBA	Benny Zeltser
13:00 - 13:45	RingHopper – Hopping from User-space to God Mode	Jonathan Lusky,Benny Zelt . . .
14:00 - 15:15	Contest Closing Ceremonies & Awards	Grifter
14:00 - 14:45	Solana JIT: Lessons from fuzzing a smart-contract . . .	Thomas Roth
15:30 - 17:30	DEF CON Closing Ceremonies & Awards	The Dark Tangent

[Return to Index](#)

## DDV - Data Duplication Village

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

Sched Page: <https://dcddv.org/dc30-talk-schedule>

DC Discord Chan: <https://discord.com/channels/708208267699945503/732732641694056478>

PDT Times	Title	speaker
Thursday		
16:00 - 18:59	DDV starts accepting drives for duplication	
Friday		
10:00 - 16:59	DDV open and accepting drives for duplication	
13:00 - 13:59	How long do hard drives and SSDs live, and what ca . . .	Andrew Klein
15:00 - 15:59	No bricks without clay - Data Fusion and Duplicati . . .	Lior Kolnik
Saturday		
10:00 - 16:59	DDV open and accepting drives for duplication	
Sunday		
10:00 - 10:59	Last chance to pick up drives at the DDV	

[Return to Index](#)

# DL - DEF CON DemoLabs

Home Page: <https://forum.defcon.org/node/239774>

PDT Times	Title	speaker
Friday		
10:00 - 11:55	TheAllCommander	Matthew Handy
10:00 - 11:55	Access Undenied on AWS	Noam Dahan
10:00 - 11:55	Vajra - Your Weapon To Cloud	Raunak Parmar
10:00 - 11:55	FISSURE: The RF Framework	Christopher Poore
10:00 - 11:55	Zuthaka: A Command & Controls (C2s) integration fr . . .	Lucas Bonastre,Alberto He . . .
12:00 - 13:55	Packet Sender	Dan Nagle
12:00 - 13:55	Wakanda Land	Stephen Kofi Asamoah
12:00 - 13:55	AzureGoat: Damn Vulnerable Azure Infrastructure	Rachna Umraniya,Nishant S . . .
12:00 - 13:55	EMBA - Open-Source Firmware Security Testing	Pascal Eckmann,Michael Me . . .
12:00 - 13:55	Mercury	David McGrew,Brandon Enri . . .
14:00 - 15:55	CyberPeace Builders	Adrien Ogee
14:00 - 15:55	AWSGoat : A Damn Vulnerable AWS Infrastructure	Sanjeev Mahunta,Jeswin Ma . . .
14:00 - 15:55	AADInternals: The Ultimate Azure AD Hacking Toolki . . .	Nestori Syynimaa
14:00 - 15:55	PCILeech and MemProcFS	Ian Vitek,Ulf Frisk
14:00 - 15:55	Badrats: Initial Access Made Easy	Kevin Clark,Dominic "Cr . . .
Saturday		
10:00 - 11:55	Empire 4.0 and Beyond	Vincent "Vinnybod" Rose,A . . .
10:00 - 11:55	Memfini - A systemwide memory monitor interface fo . . .	Shubham Dubey,Rishal Dwiv . . .
10:00 - 11:55	svachal + machinescli	Ankur Tyagi
10:00 - 11:55	Injectyll-HIDE: Pushing the Future of Hardware Imp . . .	Jonathan Fischer,Jeremy M . . .
10:00 - 11:55	EDR detection mechanisms and bypass techniques wit . . .	Maxime Meignan,Thomas Dio . . .
12:00 - 13:55	alsanna	Jason Johnson
12:00 - 13:55	unblob - towards efficient firmware extraction	Quentin Kaiser,Florian Lu . . .
12:00 - 13:55	PMR - PT & VA Management & Reporting	Abdul Alanazi,Musaed Bin . . .
12:00 - 13:55	Defensive 5G	Ryan Ashley,Eric Mair
12:00 - 13:55	SharpSCCM	Chris Thompson,Duane Mich . . .
14:00 - 15:55	OpenTDF	Paul Flynn,Cassandra Bail . . .
14:00 - 15:55	Control Validation Compass – Threat Modeling Aid . . .	Scott Small
14:00 - 15:55	ResidueFree	Logan Arkema
14:00 - 15:55	hls4ml - Open Source Machine Learning Accelerators . . .	Ben Hawks,Andres Meza
14:00 - 15:55	Xavier Memory Analysis Framework	Solomon Sonya

[Return to Index](#)

## HHV - Hardware Hacking and Soldering Skills Village

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

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

DC Discord Chan: <https://discord.com/channels/708208267699945503/732728536149786665>

---

PDT Times	Title	speaker
Friday		
10:00 - 17:59	Solder Skills Village - Open	
10:00 - 10:45	Uwb Security Primer: Rise Of A Dusty Protocol	Göktay Kaykusuz
10:00 - 17:59	Hardware Hacking Village - Open	
11:00 - 11:45	From Zero To Sao ... Or, How Far Does This Rabbit . . .	Bradán Lane
13:00 - 13:45	Reversing An M32C Firmware – Lesson Learned From . . .	Philippe Laulheret
14:00 - 14:45	Movie-Style Hardware Hacking	Bryan C. Geraghty
15:00 - 15:45	Injectyll-Hide: Build-Your-Own Hardware Implants	Jeremy Miller, Jonathan Fi . . .
Saturday		
10:00 - 17:59	Solder Skills Village - Open	
10:00 - 17:59	Hardware Hacking Village - Open	
13:00 - 13:45	RoboSumo	
16:00 - 16:30	Prizes announced for HHV Rube Goldberg Machine, Ma . . .	
Sunday		
10:00 - 12:59	Solder Skills Village - Open	
10:00 - 12:59	Hardware Hacking Village - Open	

---

[Return to Index](#)

## HRV - Ham Radio Village

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

DC Discord Chan: <https://discord.com/channels/708208267699945503/732733631667372103>

---

PDT Times	Title	speaker
Friday		
11:30 - 12:30	Your Amateur Radio License and You	Justin/InkRF
13:00 - 15:59	Free Amateur Radio License Exams	
15:00 - 15:59	Hacking Ham Radio: Dropping Shells at 1200 Baud	Rick Osgood
Saturday		
11:00 - 16:59	Free Amateur Radio License Exams	

**PDT Times**

11:30 - 11:59 Ham Nets 101  
13:00 - 13:30 Getting on the air: My experiences with Ham radio . . .  
15:00 - 15:30 Panel: Ask-a-ham

## Sunday

11:00 - 13:59 Free Amateur Radio License Exams  
11:00 - 11:30 Oli: A Simpler Pi-Star Replacement  
12:30 - 12:59 Off the grid - Supplying your own power

**Title****speaker**

Jon Marler  
Jeremy Hong

Danny Quist  
Eric Escobar

---

[Return to Index](#)

---

**IOTV - Internet Of Things Village**

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

Sched Page: <https://www.iotvillage.org/defcon.html>

DC Discord Chan: <https://discord.com/channels/708208267699945503/732734565604655114>

---

**PDT Times****Title****speaker**

## Thursday

00:00 - 15:59 IoT Village CTF Creator's Contest

## Friday

10:00 - 17:59 Hands on Hardware Hacking – eMMC to Root

Deral Heiland

10:00 - 17:59 Drone Hack

10:00 - 17:59 IoT Village CTF

10:00 - 17:59 IoT Village CTF Challenges

10:00 - 17:59 Hands on hacking labs

11:30 - 11:59 Hacking Product Security Interviews

11:00 - 11:30 Hacking Product Security Interviews

## Saturday

10:00 - 17:59 Hands on Hardware Hacking – eMMC to Root

Deral Heiland

10:00 - 17:59 Drone Hack

10:00 - 17:59 IoT Village CTF

10:00 - 13:59 BURP Suite, Forensics Tools & 0-day Exploit Develop . . .

Ken Pyle

10:00 - 17:59 IoT Village CTF Challenges

10:00 - 17:59 Hands on hacking labs

## Sunday

10:00 - 12:59 Hands on Hardware Hacking – eMMC to Root

Deral Heiland

10:00 - 12:59 Drone Hack

10:00 - 12:59 IoT Village CTF

10:00 - 12:59 IoT Village CTF Challenges

PDT Times

10:00 - 12:59 Hands on hacking labs

---

Title

speaker

[Return to Index](#)

---

## LPV - Lock Pick Village

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

DC Discord Chan: <https://discord.com/channels/708208267699945503/732734164780056708>

---

PDT Times

Title

speaker

Friday

- 10:15 - 10:45 Intro to Lockpicking  
11:00 - 11:30 Medeco cam lock exploit "an old attack made new ag . . .  
12:00 - 12:30 The least secure biometric lock on Earth?  
13:00 - 13:30 Intro to Lockpicking  
14:00 - 14:59 The Right Way To Do Wrong: Physical security secre . . .  
15:30 - 15:45 Handcuffs and how they work  
16:00 - 16:30 Intro to Lockpicking

TOOOL  
N thing  
Seth Kintigh  
TOOOL  
Patrick McNeil  
Steven Collins  
TOOOL

Saturday

- 10:15 - 10:45 Intro to Lockpicking  
11:00 - 11:30 Metal and Fire... Copying Keys via Mold and Cast T . . .  
12:00 - 13:59 Dozier Drill Tournament  
13:00 - 13:30 Intro to Lockpicking  
14:00 - 14:59 Please deposit 30c: A history of payphone locks th . . .  
16:00 - 16:30 Intro to Lockpicking

TOOOL  
Deviant Ollam  
TOOOL  
N thing  
TOOOL

Sunday

- 10:15 - 10:45 Intro to Lockpicking  
11:00 - 11:45 Safecracking for Everyone  
12:00 - 12:25 Doors, Cameras, and Mantraps. Oh, my!  
13:00 - 13:30 Intro to Lockpicking  
14:00 - 14:20 The "Why" of Lock Picking

TOOOL  
Jared Dygert  
Dylan Baklor  
TOOOL  
Christopher Forte (isaidn . . .

[Return to Index](#)

---

## MIV - MisInformation Village

Home Page: <https://defcon.misinfocon.com/>

PDT Times	Title	speaker
Friday		
10:00 - 11:30	The hybrid strategies of autocratic states: narrat . . .	Carlos Galán
11:30 - 13:30	Dazed and Seriously Confused: Analysis of Data Voi . . .	Rhyner Washburn
11:30 - 13:30	Detecting the "Fake News" Before It Was Even Writt . . .	Preslav Nakov
11:30 - 13:30	Examining the urgency of gendered health misinform . . .	Jenna Sherman
11:30 - 13:30	Cognitive Security: Human Vulnerabilities, Exploi . . .	Matthew Canham
11:30 - 13:30	SimPPL: Simulating Social Networks and Disinformat . . .	Swapneel Mehta
11:30 - 13:30	Uncovering multi-platform misinformation campaigns . . .	Zhouhan Chen
14:30 - 15:59	Fireside Chat	Adam Hickey,Jennifer Math . . .
14:30 - 15:59	FARA and DOJ's Approach to Disinformation	Adam Hickey
14:30 - 15:59	Multi-Stakeholder Online Harm Threat Analysis	Jennifer Mathieu
16:00 - 16:59	History of the weaponization of social media	Gina Rosenthal
16:00 - 16:59	Tracking Scams and Disinformation by Hacking Link . . .	Justin Rhinehart,Sam Curr . . .
16:00 - 16:59	History of Russian Cyber & Information Warfare (20 . . .	Ryan Westman
16:00 - 16:59	Information Confrontation 2022 - A loud war and a . . .	Luke Richards
Saturday		
10:45 - 12:30	Mass Disinformation Operations - How to detect and . . .	Paula González Nagore
10:00 - 10:45	Tools for Fighting Disinformation	Preslav Nakov
12:30 - 13:45	Cognitive Security in Theory and Practice	Sara-Jayne Terp
14:15 - 14:45	404! Memory Holing and the SEO Warping of Human Hi . . .	Arikia Millikan
14:45 - 15:15	Web Monetization: A privacy-preserving and open wa . . .	Uchi Uchibeke
15:15 - 15:45	Fireside Chat	Arikia Millikan,Uchi Uchi . . .
15:45 - 16:15	Ad it up: To minimize mis- and dis-information, we . . .	Jessica Dheere
16:15 - 16:45	Not Feeling Yourself: User Spoofing and Other Disi . . .	Erica Burgess

[Return to Index](#)

## PLV - Policy Village

Sched Page: <https://forum.defcon.org/node/242912>

PDT Times	Title	speaker
Friday		
12:00 - 13:45	Hacking law is for hackers - how recent changes to . . .	Leonard Bailey,Harley Gei . . .
14:00 - 15:45	Defense Through a TAC (Technical Advisory Committe . . .	The Dark Tangent
16:00 - 17:45	Election Security Bridge Building	Jack Cable,Trevor Timmons . . .

PDT Times	Title	speaker
16:00 - 17:45	Moving Regulation Upstream - An Increasing focus o . . .	Jen Ellis,Irfan Hemani,Ad . . .
19:00 - 19:59	Meet the Feds: CISA Edition (Lounge)	CISA Staff
20:00 - 21:59	Meet the Feds: DHS Edition (Lounge)	DHS Staff
Saturday		
10:00 - 11:45	Hacking Operational Collaboration	David Forscye
10:00 - 11:45	Imagining a cyber policy crisis: Storytelling and . . .	Winnona DeSombre,Safa Sha . . .
12:00 - 13:45	Hacking Aviation Policy	Timothy Weston,Ayan Islam . . .
12:00 - 13:45	Addressing the gap in assessing (or measuring) the . . .	Adrien Ogee
14:00 - 15:45	Confronting Reality in Cyberspace: Foreign Policy . . .	Neal Pollard,Jason Healey
14:00 - 15:45	Return-Oriented Policy Making for Open Source and . . .	Trey Herr,Eric Mill,Harry . . .
16:00 - 17:45	International Government Action Against Ransomware	Adam Dobell,Irfan Hemani, . . .
19:00 - 21:59	Do No Harm (Lounge)	Seeyew Mo,Jessica Wilkers . . .
Sunday		
10:00 - 11:45	Improving International Vulnerability Disclosure: . . .	Stewart Scott,Christopher . . .
10:00 - 11:45	Better Policies for Better Lives: Hacker Input to . . .	Peter Stevens
12:00 - 13:45	Offensive Cyber Industry Roundtable	Sophia D'Antoine,Winnona . . .
12:00 - 13:45	Protect Our Pentest Tools! Perks and Hurdles in Di . . .	

[Return to Index](#)

## PT - Paid Training

Home Page: <https://defcontrainings.myshopify.com/collections/all>

PDT Times	Title	speaker
Monday		
09:00 - 16:59	TCP/IP Deep Dive for Ethical Hackers – Featuring . . .	Chris Greer
09:00 - 16:59	Offensive IoT Exploitation	Trevor Stevado,Trevor Hou . . .
09:00 - 16:59	Customizable Binary Analysis: Using angr to its fu . . .	Audrey Dutcher,Fish Wang
09:00 - 16:59	A Practical Approach to Breaking & Pwning Kubernet . . .	Madhu Akula
09:00 - 16:59	Pragmatic API Exploration	Aubrey Labuschagne (Willi . . .
09:00 - 16:59	Defender's Guide to Securing Public Cloud Infrastr . . .	Abhinav Singh

**PDT Times**

	Title
09:00 - 16:59	Practical Secure Code Review
09:00 - 16:59	Zero 2 Emulated Criminal: Intro to Windows Malware . . .

Tuesday

09:00 - 16:59	TCP/IP Deep Dive for Ethical Hackers – Featuring . . .
09:00 - 16:59	Offensive IoT Exploitation
09:00 - 16:59	Customizable Binary Analysis: Using angr to its fu . . .
09:00 - 16:59	A Practical Approach to Breaking & Pwning Kubernetes . . .
09:00 - 16:59	Pragmatic API Exploration
09:00 - 16:59	Defender's Guide to Securing Public Cloud Infrastr . . .
09:00 - 16:59	Practical Secure Code Review
09:00 - 16:59	Zero 2 Emulated Criminal: Intro to Windows Malware . . .

**speaker**

Seth Law,Ken Johnson
Dahvid Schloss

Chris Greer

Trevor Stevado,Trevor Hou . . .

Audrey Dutcher,Fish Wang

Madhu Akula

Aubrey Labuschagne (Willi . . .)

Abhinav Singh

Seth Law,Ken Johnson

Dahvid Schloss

[Return to Index](#)**PWV - Password Village**Home Page: <https://passwordvillage.org/>Sched Page: <https://passwordvillage.org/schedule.html>DC Discord Chan: <https://discord.com/channels/708208267699945503/732733760742621214>**PDT Times**

Friday

	Title
13:00 - 12:59	Hacking Hashcat

**speaker**

Ray "Senpai" Morris

Saturday

11:00 - 10:59	So long, PBKDF2! The end of password-based key der . . .
---------------	--

Vivek Nair

[Return to Index](#)**RHV - Retail Hacking Village**Home Page: <https://retailhacking.store/>Sched Page: <https://retailhacking.store/schedule.html>**PDT Times**

Friday

	Title
11:00 - 11:59	Rock the Cash Box

**speaker**

Spicy Wasabi

**PDT Times****Title****speaker**

15:00 - 15:59 Mitigating vulnerabilities in two-factor authentic . . . Larsbodian

Saturday

11:00 - 11:59 Ethical considerations in using digital footprints . . . Larsbodian

---

[Return to Index](#)**SKY - SkyTalks - 303**Home Page: <https://skytalks.info/>Sched Page: <https://skytalks2022.busyconf.com/schedule>

---

**PDT Times****Title****speaker**

Friday

09:30 - 10:20 Combatting sexual abuse with threat intelligence t . . . Aaron DeVera

10:35 - 11:25 Hundreds of incidents, what can we share? Brenton Morris,Guy Barnha . . .

11:40 - 11:59 Android, Birthday Cake, Open Wifi... Oh my! A.Krontab

12:10 - 12:30 The Richest Phisherman in Colombia Matt Mosley,Nick Ascoli

12:45 - 13:35 Taking Down the Grid Joe Slowik

13:50 - 14:40 Don't Blow A Fuse: Some Truths about Fusion Centr . . . 3ncr1pt3d

14:55 - 15:45 Cloud Threat Actors: No longer cryptojacking for f . . . Nathaniel Quist

16:00 - 16:50 Automated Trolling for Fun and No Profit burninator

17:05 - 17:55 Deadly Russian Malware in Ukraine Chris Kubecka

Saturday

09:30 - 10:20 Confessions of a CISO Laura Whitt-Winyard

10:35 - 11:25 What your stolen identity did on its CoViD vacatio . . . Judge Taylor

11:40 - 12:30 This one time, at this Hospital, I got Ransomware Eirick Luraas

12:45 - 13:35 Voter Targeting, Location Data, and You 10ngrange

13:50 - 15:40 INTERNET WARS 2022: These wars aren't just virtual Jivesx,Russ Handorf,Chris . . .

16:00 - 16:50 Dancing Around DRM Game Tech Chris, . . .

17:05 - 17:55 Coming Home to Def Con: A Deep Dive into the Real . . . Richard Thieme

Sunday

09:30 - 10:20 Eradicating Disease With BioTerrorism Mixæl S. Laufer

10:35 - 11:25 Basic Blockchain Forensics K1ng\_Cr4b

11:40 - 13:30 Abortion Tech Maggie Mayhem

---

[Return to Index](#)

## SOC - Social Activities: Parties/Meetups

PDT Times	Title	speaker
Thursday		
09:00 - 17:59	Chillout Lounge - Entertainment	Rusty,s1gns0fl1fe,Pie & D . . .
12:00 - 11:59	Friends of Bill W	
16:00 - 17:59	Queercon Mixer	
16:00 - 21:59	Toxic BBQ	
17:00 - 16:59	Friends of Bill W	
18:00 - 01:59	Thursday Opening Party - Entertainment	FuzzyNop,Archwisp,DJ St3r . . .
18:00 - 20:59	DC702 Pwnagotchi Party	
21:00 - 01:59	Hallway Monitor Party - Entertainment	Tavoo,PankleDank,Heckseve . . .
Friday		
06:00 - 05:59	DEF CON Bike Ride "CycleOverride"	
09:00 - 17:59	Chillout Lounge - Entertainment	Rusty,s1gns0fl1fe,Pie & D . . .
11:00 - 10:59	No Starch Press - Book Signing - Craig Smith, The . . .	
12:00 - 11:59	No Starch Press - Book Signing - Jasper van Wouden . . .	
12:00 - 11:59	Friends of Bill W	
13:00 - 12:59	No Starch Press - Book Signing - Fotios Chantzis, . . .	
14:00 - 13:59	No Starch Press - Book Signing - Travis Goodspeed, . . .	
15:30 - 16:30	EFF: Reproductive Justice in the Age of Surveillance . . .	
16:00 - 17:59	Queercon Mixer	
16:00 - 18:59	DC404/DC678/DC770/DC470 (Atlanta Metro) Meetup	
16:00 - 18:59	DEF CON Holland DC3115 & DC3120 Group Meetup	
17:00 - 19:59	Meet the Digital Lab at Consumer Reports	
17:00 - 19:59	EFF Tech Trivia	
17:00 - 16:59	Friends of Bill W	
18:30 - 21:30	Girls Hack Village Meetup	
18:00 - 01:59	Black & White Ball - Entertainment	Magician Kody Hildebrand, . . .
18:00 - 17:59	Lawyers Meet	
19:30 - 01:59	Hacker Karaoke	
20:00 - 23:59	Movie Night Double Feature - Arrival & Real Genius	
20:00 - 21:59	Hacker Jeopardy	
20:00 - 21:59	Pilots and Hackers Meetup	
20:00 - 22:59	BlueTeam Village Party	
21:00 - 01:59	GOTHCON (#DCGOTHCON)	
21:00 - 01:59	Hallway Monitor Party - Entertainment	DJ UNIT 77 [ 0077 : 0077 . . .
22:00 - 00:59	Queercon Party	
Saturday		
09:00 - 17:59	Chillout Lounge - Entertainment	Rusty,s1gns0fl1fe,Pie & D . . .

PDT Times	Title	speaker
12:00 - 11:59	No Starch Press - Book Signing - Corey Ball, Hacki . . .	
12:00 - 11:59	Friends of Bill W	
13:00 - 12:59	No Starch Press - Book Signing - Joe Gray, Practic . . .	
14:00 - 13:59	No Starch Press - Book Signing - Jon DiMaggio, The . . .	
16:00 - 17:59	Queercon Mixer	
17:00 - 18:59	Denial, Deception, and Drinks with Mitre Engage	
17:00 - 16:59	Friends of Bill W	
18:00 - 01:59	Night of the Ninjas - Entertainment	Scotch and Bubbles,TAIKOP . . .
19:30 - 00:59	BlanketFort Con	
19:30 - 01:59	Hacker Karaoke	
20:00 - 23:59	Movie Night Double Feature - The Conversation & Th . . .	
20:30 - 23:59	Girls Hack Village 90's House Party	
20:00 - 21:59	Meet the EFF	
20:00 - 21:59	Hacker Flairgrounds	
20:00 - 21:59	Hacker Jeopardy	
21:00 - 23:59	Arcade Party	
21:00 - 01:59	VETCON	
21:00 - 01:59	Hallway Monitor Party - Entertainment	Yesterday & Tomorrow,Terr . . .
22:00 - 23:59	Whose Slide Is It Anyway? (WSIIA)	
Sunday		
09:00 - 14:59	Chillout Lounge - Entertainment	Merin MC,Pie & Darren,Rus . . .
12:00 - 11:59	Friends of Bill W	

[Return to Index](#)

## WS - DEF CON Workshops

Home Page: <https://forum.defcon.org/node/239773>

PDT Times	Title	speaker
Thursday		
10:00 - 13:59	The Purple Malware Development Approach	Olaf Hartong,Mauricio Vel . . .
10:00 - 13:59	Network Hacking 101	Victor Graf,Ben Kurtz
10:00 - 13:59	Protect/hunt/respond with Fleet and osquery	Guillaume Ross,Kathy Satt . . .
10:00 - 13:59	Hands-On TCP/IP Deep Dive with Wireshark - How thi . . .	Chris Greer
15:00 - 18:59	Introduction to Software Defined Radios and RF Hac . . .	Rich
15:00 - 18:59	Pentesting Industrial Control Systems 101: Capture . . .	Arnaud Soullie,Alexandrin . . .
15:00 - 18:59	House of Heap Exploitation	Nathan Kirkland,Maxwell D . . .
15:00 - 18:59	Introduction to Azure Security	Nishant Sharma,Jeswin Mat . . .

PDT Times	Title	speaker
Friday		
10:00 - 13:59	CICD security: A new eldorado	Remi Escourrou,Gauthier S ...
10:00 - 13:59	Finding Security Vulnerabilities Through Fuzzing	Hardik Shah
10:00 - 13:59	Introduction to Cryptographic Attacks	Matt Cheung
10:00 - 13:59	The Art of Modern Malware Analysis: Initial Infect ...	Aaron Rosenmund,Ryan J Ch ...
10:00 - 13:59	DFIR Against the Digital Darkness: An Intro to For ...	Michael Register,Michael ...
15:00 - 18:59	Hacking the Metal 2: Hardware and the Evolution of ...	Eigentourist
15:00 - 18:59	Hand On Mainframe Buffer Overflows - RCE Edition	Phil Young,Jake Labelle
15:00 - 18:59	Securing Industrial Control Systems from the core: ...	Arnaud Soullie,Alexandrin ...
15:00 - 18:59	FROM ZERO TO HERO IN A BLOCKCHAIN SECURITY	Roman Zaikin,Dikla Barda, ...
15:00 - 18:59	Securing Smart Contracts	Irvin Lemus,Kaitlyn Handl ...
Saturday		
10:00 - 13:59	Pivoting, Tunneling, and Redirection Master Class	Barrett Darnell,Wesley Th ...
10:00 - 13:59	Master Class: Delivering a New Construct in Advanc ...	Solomon Sonya
10:00 - 13:59	Dig Dug: The Lost Art of Network Tunneling	Elijah,Cam
10:00 - 13:59	Windows Defence Evasion and Fortification Primitiv ...	Rohan Durve,Paul Lainé
10:00 - 13:59	CTF 101: Breaking into CTFs (or "The Petting Zoo ...	Robert Fitzpatrick,Chris ...
15:00 - 18:59	Hybrid Phishing Payloads: From Threat-actors to Yo ...	Magnus Stubman,Jon Christ ...
15:00 - 18:59	Creating and uncovering malicious containers.	Adrian Wood,Griffin Franc ...
15:00 - 18:59	Evading Detection: A Beginner's Guide to Obfuscati ...	Anthony "Cx01N" Rose,Vinc ...
15:00 - 18:59	Securing Web Apps	Elizabeth Biddlecome,Kait ...
15:00 - 18:59	Automated Debugging Under The Hood - Building A Pr ...	Sergei Frankoff,Sean Wils ...

[Return to Index](#)

## Talk/Event Descriptions

---

### BICV - Friday - 12:00-12:30 PDT

---

**Title:** "The Man" in the Middle

**When:** Friday, Aug 12, 12:00 - 12:30 PDT

**Where:** Virtual - BIC Village

**SpeakerBio:** Alexis Hancock

No BIO available

**Description:** No Description available

---

[Return to Index](#) - Add to



- ics [Calendar](#) file

**Title:** [T]OTPs are not as secure as you might believe

**When:** Friday, Aug 12, 17:30 - 17:59 PDT

**Where:** Flamingo - Vista Ballroom

**SpeakerBio:** Santiago Kantorowicz

Santiago is a Staff Security Engineer at Twilio, with 14 years of experience in cybersecurity. He worked for 6 years securing and designing OTP and TOTP products, such as Authy and Twilio Verify. He is currently dedicated to securing Twilio Voice and video products along with Twilio Edge infrastructure. He started his cybersecurity journey doing Pen Test for 5 years, and then moved to MercadoLibre to kickstart the Appsec department. During his journey he discovered passion for other topics and worked on non-security roles such as a Product Manager and as a Product Architect.

**Description:**

You likely receive OTPs (one-time-passwords) all the time, usually in the form of an SMS with a 4 to 8 digit code in it. Pretty common when you sign-in (or register) to Uber, your bank, Whatsapp, etc. The most adopted OTP size is 6 digits, and we just accept that it's hard to guess, after all it's 1 in a million chance, and leave it there. Some may wonder, what if get a new OTP after the first one expires, assuming it's another 1 in a million chance, and forget about it. When you calculate the actual chance of guessing an OTP one after the other, the odds are NOT 1 in a million. You will be surprised how the probabilities spiral once you start thinking of brute forcing OTPs one after the other, and what about parallelising the brute force among different users, the surprise is even bigger.

---

[Return to Index](#) - Add to



- ics [Calendar](#) file

---

**MIV - Saturday - 14:15-14:45 PDT**

---

**Title:** 404! Memory Holing and the SEO Warping of Human History

**When:** Saturday, Aug 13, 14:15 - 14:45 PDT

**Where:** Caesars Forum - Summit 221->236

**SpeakerBio:** Arikia Millikan , Journalist, Media Consultant

Arikia Millikan is an American journalist and editorial strategist living in Berlin. Her journalistic work showcases my dedication to deep research and the art of the interview, bringing a humanistic perspective to topics at the intersection of technology and the human mind. In the private sector, she thrives while scrutinizing complexity and unblocking communication sticking points that occur when specialists are tasked with conveying information to a general audience. Her client roster includes founders and thought leaders from fields such as biotechnology, venture capital, telemedicine, teletherapy, femtech, cybersecurity, and mixed reality media.

**Description:**No Description available

---

[Return to Index](#) - Add to



- ics [Calendar](#) file

---

**BHV - Friday - 10:30-10:59 PDT**

---

**Title:** A Capitalist approach to hospital security

**When:** Friday, Aug 12, 10:30 - 10:59 PDT

**Where:** Flamingo - Laughlin I,II,III

## **SpeakerBio:**Eirick Luraas

Eirick spends his days discovering and mitigating vulnerabilities, occasionally doing Incident Response, and once in a while tracking down bad actors. Sometimes he gets to compromise systems to show Executives that Hospitals are horribly insecure.

Eirick earned a Master's Degree in Cybersecurity, and he has spoken several times about the dangers technology creates in healthcare. Eirick helps bring awareness of the risks we are unknowingly taking every time we visit a Hospital and works every day to reduce those dangers.

Eirick grew up in Montana and lived in Panama during his military service. He bounced around a few states in the US. He recently relocated to Tucson, Az where he is rediscovering his passion for photography. You can follow Eirick on twitter @tyercel.

Twitter: [@https://twitter.com/tyercel](https://twitter.com/tyercel)

## **Description:**No Description available

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## **DC - Friday - 16:30-17:15 PDT**

---

**Title:** A dead man's full-yet-responsible-disclosure system

**When:** Friday, Aug 12, 16:30 - 17:15 PDT

**Where:** Caesars Forum - Alliance 301-309, 321 (Track 4)

## **SpeakerBio:**Yolan Romailler , Applied Cryptographer

Yolan is an applied cryptographer delving into (and mostly dwelling on) cryptography, secure coding, and other fun things. He has previously spoken at Black Hat USA, BSidesLV, Cryptovillage, NorthSec, GopherConEU and DEF CON on topics including automation in cryptography, public keys vulnerabilities, elliptic curves, post-quantum cryptography, functional encryption, open source security, and more! He notably introduced the first practical fault attack against the EdDSA signature scheme, and orchestrated the full-disclosure with code of the CurveBall vulnerability.

## **Description:**

Do you ever worry about responsible disclosure because they could instead exploit the time-to-patch to find you and remove you from the equation? Dead man switches exist for a reason...

In this talk we present a new form of vulnerability disclosure relying on timelock encryption of content: where you encrypt a message that cannot be decrypted until a given (future) time. This notion of timelock encryption first surfaced on the Cypherpunks mailing list in 1993 by the crypto-anarchist founder, Tim May, and to date there have been numerous attempts to tackle it, none have been deployed at scale, nor made available to be used in any useful way. This changes today: we're releasing a free, open-source tool that achieves this goal with proper security guarantees. We rely on threshold cryptography and decentralization of trust to exploit the existing League of Entropy (that is running a distributed, public, verifiable randomness beacon network) in order to do so. We will first cover what all of these means, we will then see how these building blocks allow us to deploy a responsible disclosure system that guarantees that your report will be fully disclosed after the time-to-patch has elapsed. This system works without any further input from you, unlike the usual Twitter SHA256 commitments to a file on your computer.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

**Title:** A few useful things to know about AI Red Teams

**When:** Saturday, Aug 13, 10:00 - 10:50 PDT

**Where:** Caesars Forum - Summit 228->236

**SpeakerBio:** Sudipto Rakshit

No BIO available

### Description:

AI Red Teams are sprouting across organizations: Microsoft, Facebook, Google, DeepMind, OpenAI, NVIDIA all have dedicated teams to secure and red team their AI systems. Even the US Government is jumping on this bandwagon. But surprisingly, unlike traditional red teams, which have an agreed upon form, function and definition, there is little agreement on AI Red Teaming. This talk synthesizes Microsoft's perspective of AI Red Team and interleaves formal and informal conversations with more than 15 different AI Red Teams across the industry and governments, as well analyzing their job postings, publications and blog posts. We ground each of the lessons in our experience of red teaming production systems.

After this talk, you will get a taste of how AI Red Teams approach the problem, grasp what AI Red Teams do, how they interact with existing security paradigms like traditional red teaming as well as emerging areas like adversarial machine learning. You will be able to assess what it takes to be successful in this field, and how you can make an impact without a PhD in Adversarial Machine learning.

---

[Return to Index](#) - Add to



- ics [Calendar](#) file

---

## PT - Monday - 09:00-16:59 PDT

---

**Title:** A Practical Approach to Breaking & Pwning Kubernetes Clusters

**When:** Monday, Aug 15, 09:00 - 16:59 PDT

**Where:** Caesars Forum

**SpeakerBio:** Madhu Akula

Madhu Akula is a pragmatic security leader and creator of Kubernetes Goat, an intentionally vulnerable by design Kubernetes Cluster to learn and practice Kubernetes Security. Also published author and cloud native security architect with extensive experience. Also, he is an active member of the international security, DevOps, and cloud native communities (null, DevSecOps, AllDayDevOps, AWS, CNCF, USENIX, OWASP, etc). Holds industry certifications like OSCP (Offensive Security Certified Professional), CKA (Certified Kubernetes Administrator), etc.

Madhu frequently speaks and runs training sessions at security events and conferences around the world including DEFCON (24, 26, 27 & 29), BlackHat (2018, 19, 21 & 22), USENIX LISA (2018, 19 & 21), SANS Cloud Security Summit 2021 & 2022, O'Reilly Velocity EU 2019, GitHub Satellite 2020, Appsec EU (2018, 19 & 22), All Day DevOps (2016, 17, 18, 19, 20 & 21), DevSecCon (London, Singapore, Boston), DevOpsDays India, c0c0n(2017, 18 & 20), Nullcon (2018, 19, 21, 22), SACON 2019, Serverless Summit, null and multiple others.

His research has identified vulnerabilities in over 200+ companies and organizations including; Google, Microsoft, LinkedIn, eBay, AT&T, WordPress, NTOP, Adobe, etc, and is credited with multiple CVEs, Acknowledgements, and rewards. He is co-author of Security Automation with Ansible2 (ISBN-13: 978-1788394512), which is listed as a technical resource by Red Hat Ansible. He is the technical reviewer for Learn Kubernetes Security, Practical Ansible2 books by Packt Pub. Also won 1st prize for building Infrastructure Security Monitoring solution at InMobi flagship hackathon among 100+ engineering teams.

Twitter: <https://twitter.com/madhuakula>

## Description:

Latest details, requirements, description, cost:

<https://defcontrainings.myshopify.com/products/madhu-akula-a-practical-approach-to-breaking-pwning-kubernetes-clusters>

Training description:

The adoption of Kubernetes use in production has increased to 83% from a survey by CNCF. Still, most security teams struggle to understand these modern technologies.

In this real-world scenario-based training, each participant will be learning Tactics, Techniques, and Procedures (TTPs) to attack and assess Kubernetes clusters environments at different layers like Supply chain, Infrastructure, Runtime, and many others. Starting from simple recon to gaining access to microservices, sensitive data, escaping containers, escalating to clusters privileges, and even its underlying cloud environments.

By end of the training, participants will be able to apply their knowledge to perform architecture reviews, security assessments, red team exercises, and pen-testing engagements on Kubernetes Clusters and Containerized environments successfully. Also, the trainer will provide step by step guide (Digital Book) with resources and references to further your learning.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## PT - Tuesday - 09:00-16:59 PDT

---

**Title:** A Practical Approach to Breaking & Pwning Kubernetes Clusters

**When:** Tuesday, Aug 16, 09:00 - 16:59 PDT

**Where:** Caesars Forum

### SpeakerBio: Madhu Akula

Madhu Akula is a pragmatic security leader and creator of Kubernetes Goat, an intentionally vulnerable by design Kubernetes Cluster to learn and practice Kubernetes Security. Also published author and cloud native security architect with extensive experience. Also, he is an active member of the international security, DevOps, and cloud native communities (null, DevSecOps, AllDayDevOps, AWS, CNCF, USENIX, OWASP, etc). Holds industry certifications like OSCP (Offensive Security Certified Professional), CKA (Certified Kubernetes Administrator), etc.

Madhu frequently speaks and runs training sessions at security events and conferences around the world including DEFCON (24, 26, 27 & 29), BlackHat (2018, 19, 21 & 22), USENIX LISA (2018, 19 & 21), SANS Cloud Security Summit 2021 & 2022, O'Reilly Velocity EU 2019, GitHub Satellite 2020, Appsec EU (2018, 19 & 22), All Day DevOps (2016, 17, 18, 19, 20 & 21), DevSecCon (London, Singapore, Boston), DevOpsDays India, c0c0n(2017, 18 & 20), Nullcon (2018, 19, 21, 22), SACON 2019, Serverless Summit, null and multiple others.

His research has identified vulnerabilities in over 200+ companies and organizations including; Google, Microsoft, LinkedIn, eBay, AT&T, WordPress, NTOP, Adobe, etc, and is credited with multiple CVEs, Acknowledgements, and rewards. He is co-author of Security Automation with Ansible2 (ISBN-13: 978-1788394512), which is listed as a technical resource by Red Hat Ansible. He is the technical reviewer for Learn Kubernetes Security, Practical Ansible2 books by Packt Pub. Also won 1st prize for building Infrastructure Security Monitoring solution at InMobi flagship hackathon among 100+ engineering teams.

Twitter: <https://twitter.com/madhuakula>

## Description:

Latest details, requirements, description, cost:

<https://defcontrainings.myshopify.com/products/madhu-akula-a-practical-approach-to-breaking-pwning-kubernetes-clusters>

Training description:

The adoption of Kubernetes use in production has increased to 83% from a survey by CNCF. Still, most security teams struggle to understand these modern technologies.

In this real-world scenario-based training, each participant will be learning Tactics, Techniques, and Procedures (TTPs) to attack and assess Kubernetes clusters environments at different layers like Supply chain, Infrastructure, Runtime, and many others. Starting from simple recon to gaining access to microservices, sensitive data, escaping containers, escalating to clusters privileges, and even its underlying cloud environments.

By end of the training, participants will be able to apply their knowledge to perform architecture reviews, security assessments, red team exercises, and pen-testing engagements on Kubernetes Clusters and Containerized environments successfully. Also, the trainer will provide step by step guide (Digital Book) with resources and references to further your learning.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## CLV - Friday - 12:10-12:30 PDT

---

**Title:** A ransomware actor looks at the clouds: attacking in a cloud-native way

**When:** Friday, Aug 12, 12:10 - 12:30 PDT

**Where:** Flamingo - Scenic Ballroom

**SpeakerBio:** Jay Chen

Jay Chen is a security researcher with Palo Alto Networks. He has extensive research experience in cloud-native, public clouds, and edge computing. His current research focuses on investigating the vulnerabilities, design flaws, and adversary tactics in cloud-native technologies. In the past, he also researched Blockchain and mobile cloud security. Jay has authored 20+ academic and industrial papers.

### Description:

Our research shows that the number of known ransomware attacks grew 85%, and the ransom demand climbed 144% (2.2M) from 2020 to 2021. The abundant data stored in the cloud make them lucrative targets for ransomware actors. Due to the fundamental difference between the cloud-native and on-premises IT infrastructure, existing ransomware will not be effective in cloud environments. Ransomware actors will need new TTPs to achieve successful disruption and extortion. What are the weaknesses that attackers are likely to exploit? What types of cloud resources are more susceptible to ransomware attacks? How may ransomware disrupt cloud workloads? This research aims to identify the possible TTPs using the knowledge of known ransomware and cloud security incidents. I will also demonstrate POC attacks that abuse a few APIs to quickly render a large amount of cloud-hosted data inaccessible. My goal is not to create fear, uncertainty, and doubt but to help clarify the risk and mitigation strategy.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## AIV - Saturday - 12:00-12:50 PDT

---

**Title:** A System for Alert Prioritization

**When:** Saturday, Aug 13, 12:00 - 12:50 PDT

**Where:** Caesars Forum - Summit 228->236

**Speakers:** Ben Gelman ,Salma Taoufiq

**SpeakerBio:** Ben Gelman

No BIO available

**SpeakerBio:** Salma Taoufiq

No BIO available

## Description:

At any moment, tens of thousands of analysts within security operations centers (SOCs) inspect security alerts to detect evidence of compromise, but the knowledge they gain in the process is often lost, siloed, or inefficiently preserved. In our talk, we'll present a machine learning prototype that leverages this forgotten knowledge, helping analysts triage malicious alerts in a feedback loop. The system learns to predict which alerts analysts will escalate, presents these alerts to analysts, and improves as analysts make decisions about these alerts. Our system is trained on real activity from hundreds of SOC analysts analyzing threats over thousands of customer environments, and it demonstrates a dramatic reduction in alert volume with minimal loss in detection rate, freeing up analysts to dive into alerts that truly matter.

In our presentation, we describe this system in transparent detail, discussing the complexity of raw data, the limitations of current approaches, and how our system can integrate into existing infrastructure, even in the presence of unstructured data and a shifting landscape of security sensors. We'll also show our system's performance in the practical defense of a diverse population of organizations and go over in-the-trenches case studies illustrating our system's strengths and weaknesses.

[Return to Index](#) - Add to



- ics [Calendar](#) file

## DL - Friday - 14:00-15:55 PDT

**Title:** AADInternals: The Ultimate Azure AD Hacking Toolkit

**When:** Friday, Aug 12, 14:00 - 15:55 PDT

**Where:** Caesars Forum - Committee Boardroom

**SpeakerBio:** Nestori Syynimaa

Dr Nestori Syynimaa (@DrAzureAD) is one of the leading Azure AD / M365 security experts globally and the developer of the AADInternals toolkit. For over a decade, he has worked with Microsoft cloud services and was awarded Microsoft Most Valuable Security Researcher for 2021. Currently, Dr Syynimaa works as a Senior Principal Security Researcher for Secureworks Counter Threat Unit and hunts for vulnerabilities full time. He has spoken at many international scientific and professional conferences, including IEEE TrustCom, Black Hat Arsenal USA and Europe, RSA Conference, and TROOPERS. Twitter: [@https://twitter.com/DrAzureAD](https://twitter.com/DrAzureAD)

## Description:

AADInternals is an open-source hacking toolkit for Azure AD and Microsoft 365, having over 14,000 downloads from the PowerShell gallery. It has over 230 different functions in 15 categories for various purposes. The most famous ones are related to Golden SAML attacks: you can export AD FS token signing certificates remotely, forge SAML tokens, and impersonate users w/ MFA bypass. These techniques have been used in multiple attacks during the last two years, including Solarigate and other NOBELIUM attacks. AADInternals also allows you to harvest credentials, export Azure AD Connect passwords and modify numerous Azure AD / Office 365 settings not otherwise possible. The latest update can extract certificates and impersonate Azure AD joined devices allowing bypassing device based conditional access rules.

<https://o365blog.com/aadinternals/> <https://attack.mitre.org/software/S0677>

Audience: Blue teamers, red teamers, administrators, wannabe-hackers, etc.

## SKY - Sunday - 11:40-13:30 PDT

---

**Title:** Abortion Tech

**When:** Sunday, Aug 14, 11:40 - 13:30 PDT

**Where:** LINQ - BLOQ

**SpeakerBio:** Maggie Mayhem

Maggie Mayhem is a former sex worker and current full spectrum doula. She has spoken previously at HOPE as well as DefCon, Skytalks, SxSW, the United Nations Internet Governance Forum, as well as many events and universities around the world. Her website is MaggieMayhem.Com.

Twitter: [@https://twitter.com/msmaggiemayhem](https://twitter.com/msmaggiemayhem)

**Description:**

In order to protect abortion access in America, it is imperative to understand what abortion is in material terms. This primer will discuss clinical and underground abortion procedures, provider opsec, targeted legislation against abortion access, how abortion access & gender affirming care are linked, and demonstrate how to build a DIY vacuum aspiration device. This talk will be presented from the perspective that abortion should be available on demand, without apology as part of a spectrum of human reproductive rights including gender affirming care and expression of sexual orientation. Providing abortions safely requires a background in healthcare that exceeds the time and content limitations of this talk. Though abortion will be discussed in practical terms, attendees will not be taught how to perform abortions.

---

## CLV - Saturday - 14:20-14:50 PDT

---

**Title:** Access Undenied on AWS - Troubleshooting AWS IAM AccessDenied Errors

**When:** Saturday, Aug 13, 14:20 - 14:50 PDT

**Where:** Flamingo - Scenic Ballroom

**SpeakerBio:** Noam Dahan

Noam Dahan is a Senior Security Researcher at Ermetic with several years of experience in embedded security. He is a graduate of the Talpiot program at the Israel Defense Forces and spent several years in the 8200 Intelligence Corps. While this is his first time presenting at DEF CON, it is not his first time in front of a crowd. Noam was a competitive debater and is a former World Debating Champion.

Twitter: [@https://twitter.com/NoamDahan](https://twitter.com/NoamDahan)

**Description:**

Access Undenied on AWS analyzes AWS CloudTrail AccessDenied events – it scans the environment to identify and explain the reasons for which access was denied. When the reason is an explicit deny statement, AccessUndenied identifies the exact statement. When the reason is a missing allow statement, AccessUndenied offers a least-privilege policy that facilitates access.

IAM is a complex system in which permission information is distributed among many sources and permission evaluation logic is complex. The tool can help both defensive and offensive security teams with this challenge.

For defenders. The need to facilitate access to teams annoyed or frustrated by access denied messages often breaks least-privilege and creates excessive permissions in the environment. AccessUndenied gives a minimal least-privilege policy suggestion and prevents this. Some users of the tool are even scaling their use by hooking AccessUndenied to a Lambda that automatically handles AccessDenied messages and sends them a slack notification with the tool's output.

For offensive teams. In AWS IAM, a Deny statement trumps any allow. Therefore even after privilege escalation to admin, certain actions can still be blocked. Offensive teams can use AccessUndenied to quickly and effectively track down these explicit deny statements to then circumvent or remove them.

Sometimes, the new and more detailed AccessDenied messages provided by AWS will be sufficient. However, this is not always the case.

Some AccessDenied messages do not provide details. Among the services with (many or exclusively) undetailed messages are: S3, SSO, EFS, EKS, GuardDuty, Batch, SQS, and many more.

When the reason for AccessDenied is an explicit deny, it can be difficult to track down and evaluate every relevant policy.

When the explicit deny is in a service control policy (SCP), one has to find every single policy in the organization that applies to the account.

When the problem is a missing allow statement, users still need to define a least-privilege policy.

Github: <https://github.com/ermetic/access-undenied-aws>

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## DL - Friday - 10:00-11:55 PDT

---

**Title:** Access Undenied on AWS

**When:** Friday, Aug 12, 10:00 - 11:55 PDT

**Where:** Caesars Forum - Caucus Boardroom

**SpeakerBio:** Noam Dahan

Noam Dahan is a Senior Security Researcher at Ermetic with several years of experience in embedded security. He is a graduate of the Talpiot program at the Israel Defense Forces and spent several years in the 8200 Intelligence Corps. While this is his first time presenting at DEF CON, it is not his first time in front of a crowd. Noam was a competitive debater and is a former World Debating Champion.

Twitter: [@https://twitter.com/NoamDahan](https://twitter.com/NoamDahan)

### Description:

Access Undenied on AWS analyzes AWS CloudTrail AccessDenied events – it scans the environment to identify and explain the reasons for which access was denied. When the reason is an explicit deny statement, AccessUndenied identifies the exact statement. When the reason is a missing allow statement, AccessUndenied offers a least-privilege policy that facilitates access.

Audience: Cloud Security, Defense.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## MIV - Saturday - 15:45-16:15 PDT

---

**Title:** Ad it up: To minimize mis- and dis-information, we must reshape the ad tech business, not regulate speech

**When:** Saturday, Aug 13, 15:45 - 16:15 PDT

**Where:** Caesars Forum - Summit 221->236

**SpeakerBio:**Jessica Dheere

Jessica Dheere is the Director of Ranking Digital Rights. She is the founder, former executive director, and board member of SMEX (<https://www.smex.org/>), the Middle East's leading digital rights research and advocacy organization. As a 2018–19 research fellow (<https://cyber.harvard.edu/people/jessica-dheere>) at the Berkman Klein Center for Internet & Society, she launched the CYRILLA Collaborative (<https://www.cyrilla.org/>). She is also a member of the 2019-20 class of Technology and Human Rights Fellow (<https://carrcenter.hks.harvard.edu/people/jessica-dheere>) at Harvard's Carr Center for Human Rights Policy. Dheere has presented at the Internet Governance Forum, the Milton Wolf Seminar on Media and Diplomacy, RightsCon, and the International Journalism Festival.

**Description:**No Description available

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## PLV - Saturday - 12:00-13:45 PDT

---

**Title:** Addressing the gap in assessing (or measuring) the harm of cyberattacks

**When:** Saturday, Aug 13, 12:00 - 13:45 PDT

**Where:** Caesars Forum - Summit 226-227 - Policy Roundtable

**SpeakerBio:**Adrien Ogee , Chief Operations Officer

Adrien is currently Chief Operations Officer at the CyberPeace Institute, a cybersecurity non-profit based in Switzerland. At the Institute, he provides cybersecurity assistance to vulnerable communities around the world. Adrien has more than 15 years of experience in various cyber crisis response roles in the private sector, the French Cybersecurity Agency (ANSSI), the European Cybersecurity Agency (ENISA), and the World Economic Forum. Adrien holds an MEng in telecommunication and information systems, an MSc in Global Security and a Master in Business Administration.

**Description:**

Through this session we propose to outline the draft methodology, so as to leverage the expertise of the audience to provide feedback and indicate interest in peer-reviewing or testing such a methodology. As well as to have an open discussion about the value of understanding harm in a cyber context.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## CPV - Sunday - 14:15-14:59 PDT

---

**Title:** AES-GCM common pitfalls and how to work around them (PRE-RECORDED)

**When:** Sunday, Aug 14, 14:15 - 14:59 PDT

**Where:** Flamingo - Vista Ballroom

**SpeakerBio:**Santiago Kantorowicz

Santiago is a Staff Security Engineer at Twilio, with 14 years of experience in cybersecurity. He worked for 6 years securing and designing OTP and TOTP products, such as Authy and Twilio Verify. He is currently dedicated to securing Twilio Voice and video products along with Twilio Edge infrastructure. He started his cybersecurity journey doing Pen Test for 5 years, and then moved to MercadoLibre to kickstart the Appsec department. During his journey he discovered passion for other topics and worked on non-security roles such as a Product Manager and as a Product Architect.

## Description:

We will talk about AES-GCM documented and largely unknown limitations on how many encryptions it can do with one key. We won't get into the cryptographic details of the algorithm, so no need to worry about that. I'll propose some workarounds to the limitations too. There is some basic math involved :)

[Return to Index](#) - Add to



- ics [Calendar](#) file

## AV - Saturday - 16:00-17:30 PDT

**Title:** AI Music Tutorial and Show

**When:** Saturday, Aug 13, 16:00 - 17:30 PDT

**Where:** Caesars Forum - Summit 228->236

**SpeakerBio:** dadabots

No BIO available

## Description:

Learn how the dadabots make their music and enjoy a performance after the tutorial.

[Return to Index](#) - Add to



- ics [Calendar](#) file

## AV - Sunday - 11:30-12:20 PDT

**Title:** AI Trojan Attacks, Defenses, and the TrojAI Competition

**When:** Sunday, Aug 14, 11:30 - 12:20 PDT

**Where:** Caesars Forum - Summit 228->236

**SpeakerBio:** Taylor Kulp-Mcdowall

No BIO available

## Description:

As the current machine learning paradigm shifts toward the use of large pretrained models fine-tuned to a specific use case, it becomes increasingly important to trust the pretrained models that are downloaded from central model repositories (or other areas of the internet). As has been well documented in the machine learning literature, numerous attacks currently exist that allow an adversary to poison or "trojan" a machine learning model causing the model to behave correctly except when dealing with a specific adversary chosen input or "trigger". This talk will introduce the threats posed by these AI trojan attacks, discuss the current types of attacks that exist, and then focus on the state of the art techniques used to both defend and detect these attacks.

As part of an emphasis on trojan detection, the talk will also cover key aspects of the TrojAI Competition

(<https://pages.nist.gov/trojai/>)—an open leaderboard run by NIST and IARPA to spur the development of better trojan detection techniques. This leaderboard provides anyone with the opportunity to run and evaluate their own trojan detectors

across large datasets of clean/poisoned AI models already developed by the TrojAI team. These datasets consist of numerous different AI architectures trained across tasks ranging from image classification to extractive question answering. They are open-source and ready for the community to use.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## **AIV - Sunday - 14:00-14:59 PDT**

---

**Title:** AI Village Closing Remarks

**When:** Sunday, Aug 14, 14:00 - 14:59 PDT

**Where:** Caesars Forum - Summit 228->236

**Speakers:**Sven Cattell,Brian Pendleton

**SpeakerBio:**Sven Cattell

No BIO available

Twitter: [@https://twitter.com/comathematician](https://twitter.com/comathematician)

**SpeakerBio:**Brian Pendleton

No BIO available

Twitter: [@https://twitter.com/yaganub](https://twitter.com/yaganub)

### **Description:**

A review of the weekend and a short discussion of the topics to look out for in the coming year.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## **AIV - Sunday - 12:30-13:20 PDT**

---

**Title:** AI Village CTF Results and Q&A

**When:** Sunday, Aug 14, 12:30 - 13:20 PDT

**Where:** Caesars Forum - Summit 228->236

**SpeakerBio:**Will Pearce

No BIO available

Twitter: [@https://twitter.com/moothax](https://twitter.com/moothax)

**Description:**No Description available

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## **AIV - Friday - 12:00-12:50 PDT**

---

**Title:** AI Village Keynote

**When:** Friday, Aug 12, 12:00 - 12:50 PDT

**Where:** Caesars Forum - Summit 228->236

**SpeakerBio:**Keith E. Sonderling

Keith E. Sonderling was confirmed by the U.S. Senate, with a bipartisan vote, to be a Commissioner on the U.S. Equal Employment Opportunity Commission (EEOC) in 2020. Until January of 2021, he served as the Commission's Vice-Chair. His term expires July of 2024.

Prior to his confirmation to the EEOC, Commissioner Sonderling served as the Acting and Deputy Administrator of the Wage and Hour Division at the U.S. Department of Labor. Before joining the Department of Labor in 2017, Commissioner Sonderling practiced Labor and Employment law in Florida. Commissioner Sonderling also serves as a Professional Lecturer in the Law at The George Washington University Law School, teaching employment discrimination.

Since joining the EEOC, one of Commissioner Sonderling's highest priorities is ensuring that artificial intelligence and workplace technologies are designed and deployed consistent with long-standing civil rights laws. Commissioner Sonderling has published numerous articles on the benefits and potential harms of using artificial intelligence-based technology in the workplace and speaks globally on these emerging issues.

Immediately before his confirmation to the EEOC, as Deputy and Acting Administrator of the U.S. Department of Labor's Wage and Hour Division, Sonderling oversaw enforcement, outreach, regulatory work, strategic planning, performance management, communications, and stakeholder engagement. The Division accomplished back-to-back record-breaking enforcement collections and educational outreach events during his tenure. The Wage and Hour Division administers and enforces federal labor laws, including the Fair Labor Standards Act, the Family and Medical Leave Act, and the labor provisions of the Immigration and Nationality Act.

Commissioner Sonderling also oversaw the development and publication of large-scale deregulatory rules and authored numerous Opinion Letters, Field Assistance Bulletins, and All Agency Memorandums. Additionally, he was instrumental in developing the Division's first comprehensive self-audit program, which collected more than \$7 million for nearly eleven thousand workers.

Before his government service, Commissioner Sonderling was a partner at one of Florida's oldest and largest law firms, Gunster. At Gunster, he counseled employers and litigated labor and employment disputes. In 2012, then-Governor Rick Scott appointed Sonderling to serve as the Chair of the Judicial Nominating Committee for appellate courts in South Florida.

Sonderling received his B.S., magna cum laude, from the University of Florida and his J.D., magna cum laude, from Nova Southeastern University.

Twitter: [@https://twitter.com/KSonderlingEEOC](https://twitter.com/KSonderlingEEOC)

**Description:**No Description available

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## **BHV - Saturday - 11:30-11:59 PDT**

---

**Title:** All information should be free (except the brain data you want to keep in your head)

**When:** Saturday, Aug 13, 11:30 - 11:59 PDT

**Where:** Flamingo - Laughlin I,II,III

**SpeakerBio:**Isabel Straw , MD

Isabel is an Emergency Doctor in London with a background in public and global health, currently pursuing a PhD in 'Artificial Intelligence (AI) in Healthcare' at University College London (UCL).

## Description:

""When Isaac\* arrived at our Emergency department in a critical condition, the last place we thought to investigate was within the Deep Brain Stimulator (DBS) inside his head. Medical device failures or 'medical hacks' are not constituents of practitioner training, and the consequences were immediately apparent as we attempted to care for the patient [1]. Isaac's recovery was due to the resetting of the DBS settings by the programmer, and not as a result of medical attention.

The use of implanted neuromodulation is increasing in both the medical and consumer space, yet the telemetric nature of these closed looped systems expose them to a range of vulnerabilities [2-4]. Unlike hacks on insulin pumps and pacemakers, there is currently no research on hacks of brain-computer interfaces [1, 5].

Interactions between hardware and neuroanatomy invoke a range of unexpected symptoms - for Isaac the DBS error induced intense emotions and motor disturbance. An understanding of these biotechnological syndromes requires expertise from computer scientists, engineers, biomedical experts and hackers who can expose system flaws. We bring this case to DEFCON to foster collaboration between the medical and hacking community, to improve the care of patients like Isaac, who present with medical emergencies resulting from technological failures.

\*Psuedonym

""

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## DC - Saturday - 12:00-12:45 PDT

---

**Title:** All Roads leads to GKE's Host : 4+ Ways to Escape

**When:** Saturday, Aug 13, 12:00 - 12:45 PDT

**Where:** Caesars Forum - Academy 401-410, 421 (Track 3)

**Speakers:**Billy Jheng,Muhammad ALifa Ramdhan

**SpeakerBio:**Billy Jheng , Security Researcher at STAR Labs

Billy Jheng is a information security researcher at STAR Labs, focusing on Hypervisor and Linux Kernel vulnerability research and exploitation, a member of the Balsn CTF team.

He participated in Pwn2Own 2021 Vancouver & Austin and was a speaker at conferences HITCON.

Twitter: [@https://twitter.com/st424204](https://twitter.com/st424204)

**SpeakerBio:**Muhammad ALifa Ramdhan , Security Researcher at STAR Labs

Muhammad Ramdhan is a security researcher at STAR Labs, currently interested on Linux Kernel, Hypervisor or Container vulnerability research and exploitation. He is also a CTF enthusiast who is currently a member of CTF team SuperGuesser focusing on binary exploitation problems.

Twitter: [@https://twitter.com/n0psledbyte](https://twitter.com/n0psledbyte)

## Description:

Container security is a prevalent topic in security research. Due to the great design and long-term effort, containers have been more and more secure. Usage of container technology is increasingly being used. Container security is a topic that has started to be discussed a lot lately.

In late 2021, Google increased the vulnerability reward program in kCTF infrastructure, which was built on top of Kubernetes and Google Container Optimized OS, with a minimum reward of \$31,337 per submission.

In this talk, we will share about how we managed to have 4 successful submissions on kCTF VRP by exploiting four Linux kernel bugs to perform container escape on kCTF cluster, we will explain some interesting kernel exploit techniques and tricks that can be used to bypass the latest security mitigation in Linux kernel. We will also share what we did wrong that causes us to nearly lose 1 of the bounty.

As of writing, there are 14 successful entries to kCTF. In this presentation, we are willing to share our full, in-depth details on the research of kCTF.

To the best of our knowledge, this presentation will be the first to talk about a complete methodology to pwn kCTF (find and exploit bugs within 0-day and 1-day) in public.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## DL - Saturday - 12:00-13:55 PDT

---

**Title:** alsanna

**When:** Saturday, Aug 13, 12:00 - 13:55 PDT

**Where:** Caesars Forum - Accord Boardroom

**SpeakerBio:** Jason Johnson

Jason has been hacking for years, getting great satisfaction from peeling back layers of abstraction. He enjoys working on network security and machine learning. He's been to two DEF CONs in the past, and loved every minute of them. He is currently employed by WithSecure and based out of upstate New York.

### Description:

alsanna is a command-line based intercepting proxy for arbitrary TCP traffic. It includes built-in support for decrypting TLS streams, and allows editing the stream as it passes over the network. It is deliberately lightweight and documented to help hackers who need to modify its behavior. This demo will include live instances of the tool which can be used by visitors, live support for anyone looking to learn how to use alsanna, and a short on-demand walkthrough for visitors, covering how the tool works and what you need to know to modify it.

Audience: Researchers, reverse engineers, pentesters, bug bounty hunters

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## ASV - Friday - 10:00-16:59 PDT

---

**Title:** Amazon Web Services Aerospace and Satellite Jam

**When:** Friday, Aug 12, 10:00 - 16:59 PDT

**Where:** Caesars Forum - Forum 112-117

### Description:

Jams are immersive engagements that encourage you to up-level your security and coding skills on AWS through the use of hands-on real-world scenarios. The scenarios have varying level of difficulty and points associated with them. Jam engagements allow you to identify strengths, areas of improvement, and the ability to work together in team or individual challenges. Participating will help you advance your cloud cyber skills, hone your problem-solving abilities, and better understand and appreciate the complex set of threat vectors that the aerospace and satellite community confront every day. You will gain experience with a wide range of AWS services in a series of prepared scenarios across aerospace and satellite

use cases and operational tasks. Come prepared to stop threat actors from laterally moving through your virtual flight operations center. Detect manipulated imagery in your satellite imagery analysis pipeline. Defend against a DDOS attack on your satellite ground station receiver network. Harden your virtual twin Mars rover against Internet of Things (IoT) attacks. There's never a dull moment to work in space!

Required gear: Laptop and connection required to access the jam environment, set up DEF CON WiFi in advance!

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## ASV - Saturday - 10:00-16:59 PDT

---

**Title:** Amazon Web Services Aerospace and Satellite Jam

**When:** Saturday, Aug 13, 10:00 - 16:59 PDT

**Where:** Caesars Forum - Forum 112-117

### Description:

Jams are immersive engagements that encourage you to up-level your security and coding skills on AWS through the use of hands-on real-world scenarios. The scenarios have varying level of difficulty and points associated with them. Jam engagements allow you to identify strengths, areas of improvement, and the ability to work together in team or individual challenges. Participating will help you advance your cloud cyber skills, hone your problem-solving abilities, and better understand and appreciate the complex set of threat vectors that the aerospace and satellite community confront every day. You will gain experience with a wide range of AWS services in a series of prepared scenarios across aerospace and satellite use cases and operational tasks. Come prepared to stop threat actors from laterally moving through your virtual flight operations center. Detect manipulated imagery in your satellite imagery analysis pipeline. Defend against a DDOS attack on your satellite ground station receiver network. Harden your virtual twin Mars rover against Internet of Things (IoT) attacks. There's never a dull moment to work in space!

Required gear: Laptop and connection required to access the jam environment, set up DEF CON WiFi in advance!

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## DC - Saturday - 12:30-13:15 PDT

---

**Title:** Analyzing PIPEDREAM: Challenges in testing an ICS attack toolkit.

**When:** Saturday, Aug 13, 12:30 - 13:15 PDT

**Where:** Caesars Forum - Alliance 301-309, 321 (Track 4)

### SpeakerBio:Jimmy Wylie , Principal Malware Analyst II , Dragos, Inc.

Jimmy Wylie is a Principal Malware Analyst at Dragos, Inc. who spends his days (and nights) searching for and analyzing threats to critical infrastructure. He was the lead analyst on PIPEDREAM, the first ICS attack "utility belt", TRISIS, the first malware to target a safety instrumented system, and analysis of historical artifacts of the CRASHOVERRIDE attack, the first attack featuring malware specifically tailored to disrupt breakers and switchgear in an electric transmission substation.

Jimmy has worked for various DoD contractors, leveraging a variety of skills against national level adversaries, including network analysis, dead disk and memory forensics, and software development for detection and analysis of malware. After leaving the DoD contracting world, he joined Focal Point Academy, where he developed and taught malware analysis courses to civilian and military professionals across the country. In his off-time, Jimmy enjoys learning about operating systems internals, playing pool, cheap beer, and good whiskey.

## Description:

Identified early in 2022, PIPEDREAM is the seventh-known ICS-specific malware and the fifth malware specifically developed to disrupt industrial processes. PIPEDREAM demonstrates significant adversary research and development focused on the disruption, degradation, and potentially, the destruction of industrial environments and physical processes.

PIPEDREAM can impact a wide variety of PLCs including Omron and Schneider Electric controllers. PIPEDREAM can also execute attacks that take advantage of ubiquitous industrial protocols, including CODESYS, Modbus, FINS, and OPC-UA.

This presentation will summarize the malware, and detail the difficulties encountered during the reverse engineering and analysis of the malware to include acquiring equipment and setting up our lab. This talk will also release the latest results from Drago's lab including an assessment of the breadth of impact of PIPEDREAM's CODESYS modules on equipment beyond Schneider Electric's PLCs, testing Omron servo manipulation, as well as OPC-UA server manipulation. While a background in ICS is helpful to understand this talk, it is not required. The audience will learn about what challenges they can expect to encounter when testing ICS malware and how to overcome them.

---

[Return to Index](#) - Add to



- ics [Calendar file](#)

---

## SKY - Friday - 11:40-11:59 PDT

---

**Title:** Android, Birthday Cake, Open Wifi... Oh my!

**When:** Friday, Aug 12, 11:40 - 11:59 PDT

**Where:** LINQ - BLOQ

**SpeakerBio:** A.Krontab

Software Engineer by profession, lock picker and wanna be hacker by hobby. Also a Wil Wheaton look alike that actually fooled someone at DEFCON 23.

Twitter: [@https://twitter.com/akrotos](https://twitter.com/akrotos)

## Description:

What do you get when you combine a curious hacker dad at an 8 year old's birthday party with a couple open wifi networks, and a plain old android smartphone? A innocent digital trespass and spelunk into a network where full blown identity theft is possible by the end. Come hear about a low skill intrusion done with consumer hardware (No root required), apps straight off the shelf of the Google play store, and a burning curiosity and desire to get into places you're not supposed to be.  
UNPXGURCYNARG!

---

[Return to Index](#) - Add to



- ics [Calendar file](#)

---

## SOC - Saturday - 21:00-23:59 PDT

---

**Title:** Arcade Party

**When:** Saturday, Aug 13, 21:00 - 23:59 PDT

**Where:** Caesars Forum - Forum 104-105, 136

## 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 is hosted by the Military Cyber Professionals Association (a tech ed charity) and friends.

More info: [ArcadeParty.org](http://ArcadeParty.org) (open to all DEF CON attendees)

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## ASV - Friday - 15:00-15:50 PDT

---

**Title:** Ask an Airport CISO

**When:** Friday, Aug 12, 15:00 - 15:50 PDT

**Where:** Caesars Forum - Forum 112-117

**SpeakerBio:** Aakinn Patel

Aakin is the CISO of the Clark County Department of Aviation, which runs the Las Vegas International airport and 4 general aviation airports. He has worked in various CTO and cybersecurity roles going back 27 years across a wide variety of industries, and started his career as an UNIX Admin.

### Description:

In this talk, Aakin Patel goes over the unique aspects of IT and cybersecurity at an airport, what makes LAS different from most other airports. After this short overview, there will be a hosted Q&A for whatever questions people have about airport technology and airport cybersecurity.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## AI - Sunday - 10:30-11:20 PDT

---

**Title:** Attacks on Tiny Intelligence

**When:** Sunday, Aug 14, 10:30 - 11:20 PDT

**Where:** Caesars Forum - Summit 228->236

**SpeakerBio:** Yuvaraj Govindarajulu

No BIO available

### Description:

As of this year, there are over a 2.5 billion Edge-enabled IoT devices and close to 1.5 million new AI Edge devices projected to be shipped. These devices include smaller compressed versions of AI models running on them. While in the last years, we have been able to improve the performance of the AI models and reduce their memory footprint on these devices, not much has been spoken about the security threats of the AI models on tiny models.

First step towards protecting these AI models from attacks such as Model Theft, evasion and data poisoning, would be to study the efficacy of attacks on these Tiny Intelligent systems. Some of them at the lower Hardware and software layers could be protected through classical embedded security, they alone would not suffice to protect these Tiny Intelligence. Many of these tiny devices (microcontrollers) do not come with built-in security features because of their price and power requirements. So an understanding of how the core AI algorithm could be attacked and protected become necessary. In this talk we go about discussing what could be the possible threats to these devices and provide directions on how additional AI security measures would save the Tiny intelligence.

---

## BTV - Friday - 11:00-11:30 PDT

---

**Title:** Attribution and Bias: My terrible mistakes in threat intelligence attribution

**When:** Friday, Aug 12, 11:00 - 11:30 PDT

**Where:** Virtual - BlueTeam Village - Talks

### **SpeakerBio:** Seongsu Park

Seongsu Park is a passionate researcher on malware researching, threat intelligence, and incident response with over a decade of experience in cybersecurity. He has extensive experience in malware researching, evolving attack vectors researching, and threat intelligence with a heavy focus on response to nation-state adversary attacks. He's mostly tracking high-skilled Korean-speaking threat actors. Now he is working in the Kaspersky Global Research and Analysis Team(GreAT) as a Lead security researcher and focuses on analyzing and tracking security threats in the APAC region.

### **Description:**

One of the most important aspects of threat intelligence is the attribution of threat actors—identifying the entity behind an attack, their motivations, or the ultimate sponsor of the attack. Attribution is one of the most complicated aspects of cybersecurity, and it is easy to make mistakes because the underlying architecture of the internet offers numerous ways for attackers to hide their tracks. Threat actors can use false flags to deceive the security community about their identity, and natural human bias can lead researchers in the wrong direction. In this presentation, I will discuss three of the biggest lessons I've learned with regards to attribution—and how researchers can avoid making the same errors.

The first mistake is related to perception bias. The Olympic Destroyer was a cyber-sabotage attack that happened during the PyeongChang Winter Olympic in 2018. Many security vendors published information about the substance of the attack alongside unclear speculation about who was ultimately behind it. During the early stage of my Olympic Destroyer research, I strongly believed a North Korea-linked threat actor was behind the attack. Looking back, I'm overwhelmed by my confirmation bias at that time. The relationship between North Korea and South Korea was relatively stable during the Olympics, but North Korea sometimes attacked South Korea regardless. Therefore, I assumed the attack was associated with a North Korean threat actor that wanted to sow chaos during the Olympic season. However, my colleague discovered a fascinating rich header false flag designed to disguise the fact that this attack was carried out by an unrelated threat actor. Also, I confirmed that the threat actor behind this attack utilized a totally different modus operandi than the presumed North Korean threat actor after an in-depth, onsite investigation. I had allowed my perception bias to hinder my attribution efforts.

The second mistake occurred as a result of an over-reliance on third-party functions. Researchers are often inclined to rely on too many third-party tools, and occasionally this blind faith causes mistakes. One day, I discovered that one Korean-speaking threat actor utilized a 0-day exploit embedded in a Word document. Based on the metadata of the malicious document, I used Virustotal to find additional documents with similar metadata. All of them had the same language code page, which made me even more biased. From then, I started going in the wrong direction. I totally believed that those documents were created by the same threat actor. However, I later discovered that the documents were created by two different actors with very similar characteristics. Both of them are Korean-speaking actors, who, historically, attack the same target. Eventually, I uncovered the difference between the two and was able to reach the right conclusion—but this required going beyond what my tools told me was the correct answer.

The last mistake occurred as a result of impatience. When I investigated one cryptocurrency exchange incident, I noticed that the cryptocurrency trading application was compromised and had been delivered with a malicious file. Without any doubt, I concluded that the supply chain of this company was compromised, and contacted them via email to notify them of this incident. But, as soon as I contacted them, their websites went offline and the application disappeared from the website. After a closer examination of their infrastructure, I recognized that everything was fake, including the company website, application, and 24/7 support team. Later, we named this attack Operation AppleJeus, which a US-CERT also mentioned when they indicted three North Korean hackers. In my haste to conclude my research, I failed to notice an operation aspect of the operation.

Threat Intelligence is a high-profile industry with numerous stories that have major geopolitical ramifications. Not only is attribution one of the hardest aspects of this field—it's the one that carries the most significant consequences if not done correctly. Unfortunately, human intuition and bias interfere with proper attribution, leading to mistakes. By sharing my own struggles with attribution, it is my hope other researchers in the security community can carry out their own investigations with greater accuracy.

The threat intelligence industry suffers from the flow of inaccurate information. This symptom is because of irresponsible announcements and different perceptions of each vendor. In this presentation, I would like to share how we can quickly go to the wrong decisions and what attitude we need to prevent these failures.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## AIV - Friday - 09:30-10:50 PDT

---

**Title:** Automate Detection with Machine Learning

**When:** Friday, Aug 12, 09:30 - 10:50 PDT

**Where:** Caesars Forum - Summit 228->236

**SpeakerBio:**Gavin Klondike

Gavin Klondike is a senior consultant and researcher who has a passion for network security, both attack and defense. Through that passion, he runs NetSec Explained; a blog and YouTube channel which covers intermediate and advanced level network security topics, in an easy to understand way. His work has given him the opportunity to be published in industry magazines and speak at conferences such as Def Con, Def Con China, and CactusCon. Currently, he is researching into ways to address the cybersecurity skills gap, by utilizing machine learning to augment the capabilities of current security analysts.

### Description:

Today, over a quarter of security products for detection have some form of machine learning built in. However, “machine learning” is nothing more than a mysterious buzzword for many security analysts. In order to properly deploy and manage these products, analysts will need to understand how the machine learning components operate to ensure they are working efficiently. In this talk, we will dive head first into building and training our own security-related models using the 7-step machine learning process. No environment setup is necessary, but Python experience is strongly encouraged.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## AIV - Sunday - 09:00-10:20 PDT

---

**Title:** Automate Detection with Machine Learning

**When:** Sunday, Aug 14, 09:00 - 10:20 PDT

**Where:** Caesars Forum - Summit 228->236

**SpeakerBio:**Gavin Klondike

Gavin Klondike is a senior consultant and researcher who has a passion for network security, both attack and defense. Through that passion, he runs NetSec Explained; a blog and YouTube channel which covers intermediate and advanced level network security topics, in an easy to understand way. His work has given him the opportunity to be published in industry magazines and speak at conferences such as Def Con, Def Con China, and CactusCon. Currently, he is researching into ways to address the cybersecurity skills gap, by utilizing machine learning to augment the capabilities of current security analysts.

### Description:

Today, over a quarter of security products for detection have some form of machine learning built in. However, “machine learning” is nothing more than a mysterious buzzword for many security analysts. In order to properly deploy and manage these products, analysts will need to understand how the machine learning components operate to ensure they are working efficiently. In this talk, we will dive head first into building and training our own security-related models using the 7-step machine learning process. No environment setup is necessary, but Python experience is strongly encouraged.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## WS - Saturday - 15:00-18:59 PDT

---

**Title:** Automated Debugging Under The Hood - Building A Programmable Windows Debugger From Scratch (In Python)

**When:** Saturday, Aug 13, 15:00 - 18:59 PDT

**Where:** Harrah's - Silver

**Speakers:** Sergei Frankoff, Sean Wilson

**SpeakerBio:** Sergei Frankoff , Co-Founder, OpenAnalysis Inc.

Sergei is a co-founder of OpenAnalysis Inc. When he is not reverse engineering malware Sergei is focused on building automation tools for malware analysis, and producing tutorials for the OALABS YouTube channel. With over a decade in the security industry Sergei has extensive experience working at the intersection of incident response and threat intelligence.

**SpeakerBio:** Sean Wilson , Co-Founder, OpenAnalysis Inc.

Sean is a co-founder of OpenAnalysis Inc. He splits his time between reverse engineering malware and building automation tools for incident response. Sean brings over a decade of experience working in a number of incident response and application security roles with a focus on security testing and threat modelling. In his free time Sean loves fly fishing.

### Description:

How do anti-debug tricks actually work? Is there a way to automate tedious debugging tasks like unpacking malware? Have you ever wondered what is happening under the hood of a debugger?

In this workshop you will build your own programmable Windows debugger from scratch (using Python). Each component in the debugger will be built as a separate module with an accompanying lab used to explain the concepts and Windows internals that support the component. In the final lab you will have the chance to test your new debugger against various malware samples and attempt to automatically unpack them, and extract IOCs.

This workshop is aimed at malware analysts and reverse engineers who are interested in learning more about debuggers and how programmable debuggers can be used to automate some reverse engineering workflows. Students must be able to write basic Python scripts, and have a working knowledge of the Windows OS.

You will be provided with a VirtualMachine to use during the workshop. Please make sure to bring a laptop that meets the following requirements. - Your laptop must have VirtualBox or VMWare installed and working prior to the start of the course. - Your laptop must have at least 60GB of disk space free. - Your laptop must also be able to mount USB storage devices. (Make sure you have the appropriate dongle if you need one.)

### Materials

Students will be provided with a VirtualMachine to use during the workshop. They will need to bring a laptop that meets the following requirements; - The laptop must have VirtualBox or VMWare installed and working prior to class. - The laptop must have at least 60GB of disk space free. - The laptop must be able to mount USB storage devices (ensure you have the appropriate dongle if you need one).

### Prereq

Students must be able to write basic Python scripts and have a basic understanding of the Windows operating system. Familiarity with a Windows user space debugger like x64dbg would also be a benefit.

## SKY - Friday - 16:00-16:50 PDT

---

**Title:** Automated Trolling for Fun and No Profit

**When:** Friday, Aug 12, 16:00 - 16:50 PDT

**Where:** LINQ - BLOQ

**SpeakerBio:**burninator

Burninator was a software engineer before becoming an appsec redteamer in 2018, but has been hacking all the things since high school.

Twitter: [@https://twitter.com/burninatorsec](https://twitter.com/burninatorsec)

**Description:**

Having fun is at the core of discovering new CVEs or getting bug bounties. While this talk is about neither of those things, I want to show that doing something for the lulz can lead to some awesome possibilities no matter what you're doing. Would you like to troll more but you work full time? Let's automate! Are you one of the 40,000+ users who have been contacted by my bots such as the /r/pmmebot Reddit bot? Or ChinaNumberFour? Or J0hnnyDoxxille? Let's talk it out. Some may say learning to code AI in Python just to troll is too much effort. I agree. I did it anyway.

---

## CLV - Friday - 10:10-10:50 PDT

---

**Title:** Automating Insecurity in Azure

**When:** Friday, Aug 12, 10:10 - 10:50 PDT

**Where:** Flamingo - Scenic Ballroom

**SpeakerBio:**Karl Fosaaen

As a Senior Director at NetSPI, Karl leads the Cloud Penetration Testing service line and oversees NetSPI's Portland, OR office. Karl holds a BS in Computer Science from the University of Minnesota and is approaching 15 years of consulting experience in the security industry. Karl spends most of his research time focusing on Azure security and contributing to the NetSPI blog. As part of this research, Karl created the MicroBurst toolkit (<https://github.com/Netspi/Microburst>) to house many of the PowerShell tools that he uses for testing Azure. In 2021, Karl co-authored the book 'Penetration Testing Azure for Ethical Hackers' with David Okeyode. Over the years, Karl has held the Security+, CISSP, and GXPN certifications. Since DEF CON 19, Karl has spent most of his conference time selling merchandise as a Goon on the Merch (formerly SWAG) team.

Twitter: [@https://twitter.com/kfosaaen](https://twitter.com/kfosaaen)

**Description:**

Microsoft's Azure cloud platform has over 200 services available to use, so why are we picking on just one? Automation Accounts are used in almost every Azure subscription and have been the source of two different CVEs in the last year, including one issue that exposed credentials between tenants. Given the credentials and access that are often associated with Automation Accounts, they're an easy target for attackers in an Azure subscription. In this talk, we will go over how Automation Accounts function within Azure, and how attackers can abuse built-in functionality to gain access to credentials, privileged identities, and sensitive information. Furthermore, we will do a deep dive on four vulnerabilities from the last year that all apply to Azure Automation Accounts.

## DC - Saturday - 15:30-15:50 PDT

---

**Title:** Automotive Ethernet Fuzzing: From purchasing ECU to SOME/IP fuzzing

**When:** Saturday, Aug 13, 15:30 - 15:50 PDT

**Where:** Caesars Forum - Forum 104-105, 135-136 (Track 1)

**Speakers:** Woongjo choi, Soohwan Oh, Jonghyuk Song

**SpeakerBio:** Woongjo choi , Blueteam Leader, Autocrypt

Woongjo Choi is in charge of team leader of blue team and also vehicle security test engineer at Autocrypt. Also, he designed automotive security test solution and conducted the fuzzing test. Experienced in various fields : Vehicle security, Mobile phone, Application Processor, Ultrasound system, etc.

**SpeakerBio:** Soohwan Oh , Blueteam Engineer, Autocrypt

Soohwan Oh is an automotive engineer and security tester at Autocrypt blue team.

He is mainly working on fuzzing test and issue analysis on the in-vehicle networks, such as CAN/CAN-FD, UDSonCAN and Automotive Ethernet.

Also, he has designed the requirements of automotive security test solutions.

**SpeakerBio:** Jonghyuk Song , "Jonghyuk Song, Redteam Leader, Autocrypt"

Jonghyuk Song is lead for Autocrypt's Red Team. His current tasks are security testing for automotive including fuzzing, penetration testing, and vulnerability scanning.

He researches security issues in not only in-vehicle systems, but also V2G and V2X systems. Jonghyuk received his Ph.D. in Computer Science and Engineering at POSTECH, South Korea in 2015. He has worked in Samsung Research as an offensive security researcher, where his work included finding security issues in smartphones, smart home appliances and network routers.

### Description:

Car hacking is a tricky subject to hackers because it requires lots of money and hardware knowledge to research with a real car. An alternative way would be to research with an ECU but it is also difficult to know how to setup the equipment. Moreover, in order to communicate with Automotive Ethernet services running on the ECU, you need additional devices such as media converters and Ethernet adapters supporting Virtual LAN(VLAN). Even if you succeed in building the hardware environment, you can't communicate with the ECU over SOME/IP protocol of Automotive Ethernet if you don't know the network configuration, such as VLAN ID, service IDs and IP/port mapped to each service.

This talk describes how to do fuzzing on the SOME/IP services step by step. First, we demonstrate how to buy an ECU, how to power and wire it. Second, we explain network configurations to communicate between ECU and PC. Third, we describe how to find out the information required to perform SOME/IP fuzzing and how to implement SOME/IP Fuzzer. We have conducted the fuzzing with the BMW ECUs purchased by official BMW sales channels, not used products.

We hope this talk will make more people to try car hacking and will not go through the trials and errors that we have experienced.

---

## DC - Friday - 12:00-12:45 PDT

---

**Title:** Avoiding Memory Scanners: Customizing Malware to Evade YARA, PE-sieve, and More

**When:** Friday, Aug 12, 12:00 - 12:45 PDT

**Where:** Caesars Forum - Academy 401-410, 421 (Track 3)

**SpeakerBio:** Kyle Avery , Hacker

Kyle Avery has been interested in computers for his entire life. Growing up, he and his dad self-hosted game servers and ran their own websites. He focused on offensive security in university and has spent the last few years learning about malware and post-exploitation. Kyle previously worked at Black Hills Information Security as a red teamer, specializing in .NET development. He has since moved to lead an internal red team at H-E-B, where he works to improve the organization's security posture through continuous testing of configurations and processes. Before this talk, Kyle hosted BHIS and WWHF webcasts on Covert .NET Tradecraft, Abusing Microsoft Office, and Modern C2 Communications.

Twitter: [@https://twitter.com/kyleavery\\_](https://twitter.com/kyleavery_)

**Description:**

Tired of encoding strings or recompiling to break signatures? Wish you could keep PE-sieve from ripping your malware out of memory? Interested in learning how to do all of this with your existing COTS or private toolsets?

For years, reverse engineers and endpoint security software have used memory scanning to locate shellcode and malware implants in Windows memory. These tools rely on IoCs such as signatures and unbacked executable memory. This talk will dive into the various methods in which memory scanners search for these indicators and demonstrate a stable evasion technique for each method. A new position-independent reflective DLL loader, AceLdr, will be released alongside the presentation and features the demonstrated techniques to evade all of the previously described memory scanners. The presenter and their colleagues have used AceLdr on red team operations against mature security programs to avoid detection successfully.

This talk will focus on the internals of Pe-sieve, MalMemDetect, Moneta, Volatility malfind, and YARA to understand how they find malware in memory and how malware can be modified to fly under their radar consistently.

---

## DL - Friday - 14:00-15:55 PDT

---

**Title:** AWSGoat : A Damn Vulnerable AWS Infrastructure

**When:** Friday, Aug 12, 14:00 - 15:55 PDT

**Where:** Caesars Forum - Caucus Boardroom

**Speakers:** Sanjeev Mahunta,Jeswin Mathai

**SpeakerBio:** Sanjeev Mahunta

Sanjeev Mahunta is a Cloud Software Engineer at INE with a strong background in web, mobile application design and has high proficiency in AWS. He holds a bachelor's degree in Computer Science from Amity University Rajasthan. He has 2+ years of experience building front-end applications for the web and implementing ERP solutions. Having interned at Defence Research and Development Organisation (DRDO), he has acquired neat skills in application development. His areas of interest include Web Application Security, Serverless Application Deployment, System Design and Cloud.

## **SpeakerBio:**Jeswin Mathai , Senior Security Researcher

Jeswin Mathai is a Senior Security Researcher at INE. Prior to joining INE, He was working as a senior security researcher at Pentester Academy (Acquired by INE). At Pentester Academy, he was also part of the platform engineering team who was responsible for managing the whole lab infrastructure. He has published his work at DEFCON China, RootCon, Blackhat Arsenal, and Demo labs (DEFCON). He has also been a co-trainer in classroom trainings conducted at Black Hat Asia, HITB, RootCon, OWASP NZ Day. He has a Bachelor degree from IIIT Bhubaneswar. He was the team lead at InfoSec Society IIIT Bhubaneswar in association with CDAC and ISEA, which performed security auditing of government portals, conducted awareness workshops for government institutions. His area of interest includes Cloud Security, Container Security, and Web Application Security.

## **Description:**

Compromising an organization's cloud infrastructure is like sitting on a gold mine for attackers. And sometimes, a simple misconfiguration or a vulnerability in web applications, is all an attacker needs to compromise the entire infrastructure. Since cloud is relatively new, many developers are not fully aware of the threatscape and they end up deploying a vulnerable cloud infrastructure. When it comes to web application pentesting on traditional infrastructure, deliberately vulnerable applications such as DVWA and bWAPP have helped the infosec community in understanding the popular web attack vectors. However, at this point in time, we do not have a similar framework for the cloud environment. In this talk, we will be introducing AWSGoat, a vulnerable by design infrastructure on AWS featuring the latest released OWASP Top 10 web application security risks (2021) and other misconfiguration based on services such as IAM, S3, API Gateway, Lambda, EC2, and ECS. AWSGoat mimics real-world infrastructure but with added vulnerabilities. The idea behind AWSGoat is to provide security enthusiasts and pen-testers with an easy to deploy/destroy vulnerable infrastructure where they can learn how to enumerate cloud applications, identify vulnerabilities, and chain various attacks to compromise the AWS account. The deployment scripts will be open-source and made available after the talk.

Audience: Cloud, Ofference, Defense

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## **DL - Friday - 12:00-13:55 PDT**

**Title:** AzureGoat: Damn Vulnerable Azure Infrastructure

**When:** Friday, Aug 12, 12:00 - 13:55 PDT

**Where:** Caesars Forum - Committee Boardroom

**Speakers:**Rachna Umraniya,Nishant Sharma

## **SpeakerBio:**Rachna Umraniya

Rachana Umraniya is a Cloud Developer at INE and has two years of experience in software development. She specializes in building applications with Java frameworks and is well versed with databases. She has a Master's degree in Computer Science from NIT Hamirpur. Her area of interest includes cloud security, cryptography, web application, and docker security.

## **SpeakerBio:**Nishant Sharma , Security Research Manager

Nishant Sharma is a Security Research Manager at INE, where he manages the development of next-generation on-demand labs. Before INE, he worked as R&D Head of Pentester Academy (Acquired by INE), where he led a team of developers/researchers to create content and platform features for AttackDefense. He has also developed multiple gadgets for WiFi pentesting/monitoring such as WiMonitor, WiNX, and WiMini. With over 9+ years of experience in development and content creation, he has conducted trainings/workshops at Blackhat Asia/USA, HITB Amsterdam/Singapore, OWASP NZ day, and DEFCON USA villages. He has presented/published his work at Blackhat USA/Asia Arsenal, DEFCON USA/China, Wireless Village, Packet Village and IoT village. He has also conducted WiFi Pentesting training at Blackhat USA 2019, 2021. He had started his career as a firmware developer at Mojo Networks (Acquired by Arista) where he worked on new features for the enterprise-grade WiFi APs and maintenance of state-of-the-art WIPS. He has a Master degree in Information Security from IIIT Delhi. He has also published peer-reviewed academic research on HMAC security. His areas of interest

include WiFi, Azure, and Container security.

## Description:

Microsoft Azure cloud has become the second-largest vendor by market share in the cloud infrastructure providers (as per multiple reports), just behind AWS. There are numerous tools and vulnerable applications available for AWS for the security professional to perform attack/defense practices, but it is not the case with Azure. There are far fewer options available to the community. AzureGoat is our attempt to shorten this gap by providing a ready-to-deploy vulnerable setup (vulnerable application + misconfigured Azure components + multiple attack paths) that can be used to learn/teach/practice Azure cloud environment pentesting.

Audience: Cloud, Ofference, Defense

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## CPV - Friday - 10:30-10:59 PDT

---

**Title:** Back to School! Hello RSA... and beyond!

**When:** Friday, Aug 12, 10:30 - 10:59 PDT

**Where:** Flamingo - Vista Ballroom

### **SpeakerBio:**Mike Guirao

Mike Guirao (a.k.a Chicolinux) is currently doing a PhD in Computer Science at the New Mexico State University, he holds a SANS GCIH 504 certification and has given a couple of workshops at previous editions of DEFCON. He is currently working at the intersection of ML and Security. He loves volunteering for the CPV!!!

## Description:

RSA is the Gold Standard for public key crypto, there is still no other algorithm known as broadly as RSA, so in this talk I will provide a deep review of RSA with even some fun math so we can grasp the fundamentals of RSA and understand its beauty. Along the way I will provide some examples with Python and command line tools in Linux! The goal of this talk is for you to fully understand how RSA works once this talk is over!

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## DC - Friday - 13:00-13:20 PDT

---

**Title:** Backdooring Pickles: A decade only made things worse

**When:** Friday, Aug 12, 13:00 - 13:20 PDT

**Where:** Caesars Forum - Academy 401-410, 421 (Track 3)

### **SpeakerBio:**ColdwaterQ , Senior Security Engineer at Nvidia

ColdwaterQ has always been interested in understanding how things work. This led to a career in the security industry and allowed him to be a part of NVIDIA's AI Red Team where he works currently. He has attended every DEF CON starting in 2012, even if the last two were only remotely, and has returned this year hoping to help give some of what he learned back to the community.

Twitter: [@https://twitter.com/ColdwaterQ](https://twitter.com/ColdwaterQ)

## Description:

Eleven years ago, "Sour Pickles" was presented by Marco Slaviero. Python does already said pickles were insecure at that

time. But since then, machine learning frameworks started saving models in pickled formats as well. So, I will show how simple it is to add a backdoor into any pickled object using machine learning models as an example. As well as an example of how to securely save a model to prevent malicious code from being injected into it.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## BTV - Sunday - 11:00-11:59 PDT

---

**Title:** Backdoors & Breaches, Back to the Stone Age!

**When:** Sunday, Aug 14, 11:00 - 11:59 PDT

**Where:** Flamingo - Savoy Ballroom - BTV Main Stage

### Description:

Don't flake early! There will be several rounds of well-punned games all localized to Project Obsidian's killchain data and the tools utilized. Learn how the fates will treat you with an incident on the line. Backdoors & Breaches is an Incident Response Card Game from Black Hills Information Security and Active Countermeasures. The game contains 52 unique cards to conduct incident response tabletop exercises and learn attack tactics, tools, and methods.

<https://www.blackhillsinfosec.com/projects/backdoorsandbreaches/>

A crowd interactive, igneous take on the BHIS IR card game.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## DL - Friday - 14:00-15:55 PDT

---

**Title:** Badrats: Initial Access Made Easy

**When:** Friday, Aug 12, 14:00 - 15:55 PDT

**Where:** Caesars Forum - Society Boardroom

**Speakers:** Kevin Clark, Dominic "Cryillic" Cunningham

### SpeakerBio:Kevin Clark

Kevin Clark is a Software Developer at Def-Logix focused on development of offensive security tools. His previous work includes Penetration Testing and Red Team Operator, focusing on initial access and active directory exploitation. Kevin contributes to open-source tools such as PowerShell Empire and publishes custom security toolkits such as Badrats and WindowsBinaryReplacements. Kevin authors a cybersecurity blog at <https://henpeebin.com/kevin/blog>.

Twitter: [@https://twitter.com/GuhnooPlusLinux](https://twitter.com/GuhnooPlusLinux)

### SpeakerBio:Dominic "Cryillic" Cunningham

Dominic "Cryillic" Cunningham is a Red Team Content Engineer for TryHackMe, a large cybersecurity education platform. He is currently pursuing a degree in computing security with a focus in digital forensics and malware. His work includes general adversary emulation, offensive operations, and evasion. He specializes in researching and documentation of Evasion Techniques, Windows Internals, and Active Directory. Most of his work and research has been published at <https://www.tryhackme.com>, where he has also developed and released numerous CTF boxes and enterprise-level ranges.

### Description:

Remote Access Trojans (RATs) are one of the defining tradecraft for identifying an Advanced Persistent Threat. The reason being is that APTs typically leverage custom toolkits for gaining initial access, so they do not risk burning full-featured

implants. Badrats takes characteristics from APT Tactics, Techniques, and Procedures (TTPs) and implements them into a custom Command and Control (C2) tool with a focus on initial access and implant flexibility. The key goal is to emulate that modern threat actors avoid loading fully-featured implants unless required, instead opting to use a smaller staged implant. Badrats implants are written in various languages, each with a similar yet limited feature set. The implants are designed to be small for antivirus evasion and provides multiple methods of loading additional tools, such as shellcode, .NET assemblies, PowerShell, and shell commands on a compromised host. One of the most advanced TTPs that Badrats supports is peer-to-peer communications over SMB to allow implants to communicate through other compromised hosts.

Audience: Offense

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## SKY - Sunday - 10:35-11:25 PDT

---

**Title:** Basic Blockchain Forensics

**When:** Sunday, Aug 14, 10:35 - 11:25 PDT

**Where:** LINQ - BLOQ

**SpeakerBio:** K1ng\_Cr4b

As a Cryptocurrency Fraud and Compliance Analyst I follow nefarious activity that occurs on the blockchain. Cases can be anything from scams, hacks, ransomware, money laundering, illicit finance, or dark web criminal activity. The field is constantly evolving, and I am excited to share with you some real life cases and other exciting findings. All information in the talk is shared in the lens of how you can better protect your privacy while using cryptocurrency and how you should respond if victimized.

### Description:

The transparency, immutability, and availability of cryptocurrency blockchain data work to the advantage of Blockchain Forensics Investigators. Follow a crytpocurrency forensic analyst as we go from a single transaction to attribution.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## PLV - Sunday - 10:00-11:45 PDT

---

**Title:** Better Policies for Better Lives: Hacker Input to international policy challenges

**When:** Sunday, Aug 14, 10:00 - 11:45 PDT

**Where:** Caesars Forum - Summit 226-227 - Policy Roundtable

**SpeakerBio:** Peter Stevens , Policy Advisor for CyberSecurity, Organisation for Economic Co-operation and Development (OECD)

No BIO available

### Description:

Every year, delivering effective cyber security policies becomes more urgent, and more complicated. These challenges are becoming more international. Just thinking about product security for IoT; consumers are buying more smart products through online marketplaces, supply chains are becoming more complex and overly reliant on online marketplaces , that often exist outside of the remit for existing legislation. Meanwhile, the vast majority of consumers simply don't know what to look for to assess security. The problem isn't just security, but it is one of market failure.

In the policy space, it also feels like there is a market failure at play. Security researchers want to feed into policy makers' approaches, and civil servants (many of whom are generalists) need technical experts to help them assess lobbying and design proportionate plans.

The OECD exists to promote 'better policies for better lives'. We support civil servants around the world, and would like to offer opportunities for the security research community to feed in at a broader scale. This will be a working session, with a particular focus on product security (including IoT) and the challenges facing the security research community in the handling of vulnerabilities.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## BHV - Friday - 10:00-10:30 PDT

---

**Title:** BioHacking Village Keynote

**When:** Friday, Aug 12, 10:00 - 10:30 PDT

**Where:** Flamingo - Laughlin I,II,III

**SpeakerBio:**Nina Alli

No BIO available

Twitter: <https://twitter.com/headinthebooth>

**Description:**No Description available

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## SOC - Friday - 18:00-01:59 PDT

---

**Title:** Black & White Ball - Entertainment

**When:** Friday, Aug 12, 18:00 - 01:59 PDT

**Where:** Caesars Forum - Forum 120-123, 129, 137

**Speakers:**Magician Kody Hildebrand,Miss Jackalope,n0x08,Skittish & Bus,Biolux,Dual Core,Icetre Normal,Keith Meyers

**SpeakerBio:**Magician Kody Hildebrand

No BIO available

**SpeakerBio:**Miss Jackalope

No BIO available

**SpeakerBio:**n0x08

No BIO available

**SpeakerBio:**Skittish & Bus

No BIO available

**SpeakerBio:**Biolux

No BIO available

## **SpeakerBio:**Dual Core

No BIO available

## **SpeakerBio:**Icetre Normal

No BIO available

## **SpeakerBio:**Keith Meyers

No BIO available

### **Description:**

18:00 - 19:00: Hildebrand Magic  
19:00 - 20:00: Dual Core  
20:00 - 21:00: Icetre Normal  
21:00 - 22:00: n0x08  
22:00 - 23:00: Skittish & Bus  
23:00 - 00:00: Biolux  
00:00 - 00:15: Costume Contest  
00:15 - 01:00: Miss Jackalope  
01:00 - 02:00: Keith Myers

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## **DC - Saturday - 17:30-18:15 PDT**

---

**Title:** Black-Box Assessment of Smart Cards

**When:** Saturday, Aug 13, 17:30 - 18:15 PDT

**Where:** Caesars Forum - Alliance 301-309, 321 (Track 4)

### **SpeakerBio:**Daniel Crowley , Head of Research, X-Force Red

Daniel Crowley is the head of research and a penetration tester for X-Force Red. Daniel denies all allegations regarding unicorn smuggling and questions your character for even suggesting it. Daniel is the primary author of both the Magical Code Injection Rainbow, a configurable vulnerability testbed, and FeatherDuster, an automated cryptanalysis tool. Daniel enjoys climbing large rocks and is TIME magazine's 2006 person of the year. Daniel has been working in the information security industry since 2004 and is a frequent speaker at conferences including Black Hat, DEF CON, Shmoocon, and SOURCE. Daniel does his own charcuterie and brews his own beer. Daniel's work has been included in books and college courses. Daniel also holds the noble title of Baron in the micronation of Sealand.

Twitter: [@https://twitter.com/dan\\_crowley](https://twitter.com/dan_crowley)

### **Description:**

You probably have at least two smart cards in your pockets right now. Your credit card, and the SIM card in your cell phone. You might also have a CAC, metro card, or the contactless key to your hotel room. Many of these cards are based on the same basic standards and share a common command format, called APDU.

This talk will discuss and demonstrate how even in the absence of information about a given card, there are a series of ways to enumerate the contents and capabilities of a card, find exposed information, fuzz for input handling flaws, and exploit poor authentication and access control.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

**Title:** BlanketFort Con

**When:** Saturday, Aug 13, 19:30 - 00:59 PDT

**Where:** Caesars Forum - Forum 109-110

### Description:

Blanket Fort 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 animal onesies!

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## BTV - Sunday - 13:00-13:59 PDT

---

**Title:** Blue Team Village Closing Ceremony

**When:** Sunday, Aug 14, 13:00 - 13:59 PDT

**Where:** Flamingo - Savoy Ballroom - BTV Main Stage

### Description:

Closing ceremony for Blue Team Village @ DEF CON 30

Closing ceremony for Blue Team Village @ DEF CON 30

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## BTV - Friday - 10:00-10:30 PDT

---

**Title:** Blue Team Village Opening Ceremony

**When:** Friday, Aug 12, 10:00 - 10:30 PDT

**Where:** Flamingo - Savoy Ballroom - BTV Main Stage

### Description:

Blue Team Village Opening Ceremony

Blue Team Village Opening Ceremony

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## BTV - Friday - 17:00-17:59 PDT

---

**Title:** Blue Teaming Cloud: Security Engineering for Cloud Forensics & Incident Response

**When:** Friday, Aug 12, 17:00 - 17:59 PDT

**Where:** Flamingo - Savoy Ballroom - BTV Main Stage

**Speakers:**KyleHaxWhy,Cassandra Young (muteki),Misstech,John Orleans

**SpeakerBio:**KyleHaxWhy

KyleHaxWhy likes bananas.

**SpeakerBio:**Cassandra Young (muteki)

Cassandra (aka muteki) works full time in information security consulting, specializing in Cloud Security Architecture and Engineering. She holds a master's degree in Computer Science, focusing on cloud-based app development and academic research on serverless security and privacy/anonymity technology. Additionally, as one of the directors of Blue Team Village, Cassandra works to bring free Blue Team talks, workshops and more to the broader security community.

Twitter: [@https://twitter.com/muteki\\_rt](https://twitter.com/muteki_rt)

**SpeakerBio:**Misstech

As part of Microsoft's customer facing Detection and Response Team (DART), I work as a cloud hunter and lead investigator, battling alongside our customers on the front lines of incident response. Our work often involves dealing with live incidents involving APT and nation state actors and hunting them is what brings me joy.

**SpeakerBio:**John Orleans

To be completed.

**Description:**

Whether you're in AWS, Azure or GCP, cloud security engineering doesn't stop at basic guardrails and sending logs to a SIEM. So how do you engineer for the challenges unique to cloud forensics and incident response? This panel of cloud security engineers and incident responders will share their experiences and insights to help you take your security engineering from "just the basics" to "prepared for the inevitable".

Whether you're in AWS, Azure or GCP, cloud security engineering doesn't stop at basic guardrails and sending logs to a SIEM. So how do you engineer for the challenges unique to cloud forensics and incident response? This panel of cloud security engineers and incident responders will share their experiences and insights to help you take your security engineering from "just the basics" to "prepared for the inevitable".

---

[Return to Index](#) - Add to

[Google Calendar](#)

- ics [Calendar](#) file

---

## SOC - Friday - 20:00-22:59 PDT

---

**Title:** BlueTeam Village Party

**When:** Friday, Aug 12, 20:00 - 22:59 PDT

**Where:** LINQ - Pool

**Description:**

This year BTV will be celebrating five years at DEF CON!!! Join us Friday night 8pm-11pm at the LINQ pool. Libations will be available at the cash bar. Free tacos, sliders, and other goodies.

Dual Core will be performing at 9pm!

We hope to see you during this special Homecoming event.

---

[Return to Index](#) - Add to

[Google Calendar](#)

- ics [Calendar](#) file

---

## ASV - Friday - 10:00-15:59 PDT

---

**Title:** Boeing ARINC 429 Airplane Challenge and CTF

**When:** Friday, Aug 12, 10:00 - 15:59 PDT

**Where:** Caesars Forum - Forum 112-117

### Description:

Boeing Test & Evaluation (T&E) has developed two modules to provide an interactive learning environment and engagement opportunity on ARINC 429 data bus. Three modules will be offered, including a 10-15 minute guided discussion on the basics of ARINC 429, highlighting the key components necessary to participate in the two interactive modules. Boeing will provide an interactive learning environment to improve situational awareness of ARINC 429 data bus and promote discussion on Cyber T&E across the aviation industry. After completing the basics guided tour, participants may engage in one or both of events, the Airplane Challenge and CTF.

In order to get participants familiar with ARINC 429 concepts, there will be a presentation introducing 429 and the challenge environment at 10:30 and 13:00 both days.

Event #1 – Airplane Challenge (“AC”): during this event the user is presented with a user interface to send their own crafted 429 messages. The participant will be assigned an airplane on a map with the objectives of navigating the airplane to a win condition.

Event #2 – Capture The Flag (CTF): The participants will connect into the CTF to take on challenges involving protocol and message manipulation. The participant will be able to validate each flag found in order to complete the event!

Required gear: for the AC, you will need a mobile phone and/or Laptop with ability to connect to WiFi. For the CTF you will need a laptop and ethernet cable

Signups: first come first serve!

---

[Return to Index](#) - Add to



- ics [Calendar](#) file

---

## ASV - Saturday - 10:00-15:59 PDT

---

**Title:** Boeing ARINC 429 Airplane Challenge and CTF

**When:** Saturday, Aug 13, 10:00 - 15:59 PDT

**Where:** Caesars Forum - Forum 112-117

### Description:

Boeing Test & Evaluation (T&E) has developed two modules to provide an interactive learning environment and engagement opportunity on ARINC 429 data bus. Three modules will be offered, including a 10-15 minute guided discussion on the basics of ARINC 429, highlighting the key components necessary to participate in the two interactive modules. Boeing will provide an interactive learning environment to improve situational awareness of ARINC 429 data bus and promote discussion on Cyber T&E across the aviation industry. After completing the basics guided tour, participants may engage in one or both of events, the Airplane Challenge and CTF.

In order to get participants familiar with ARINC 429 concepts, there will be a presentation introducing 429 and the challenge environment at 10:30 and 13:00 both days.

Event #1 – Airplane Challenge (“AC”): during this event the user is presented with a user interface to send their own crafted 429 messages. The participant will be assigned an airplane on a map with the objectives of navigating the airplane to a win

condition.

Event #2 – Capture The Flag (CTF): The participants will connect into the CTF to take on challenges involving protocol and message manipulation. The participant will be able to validate each flag found in order to complete the event!

Required gear: for the AC, you will need a mobile phone and/or Laptop with ability to connect to WiFi. For the CTF you will need a laptop and ethernet cable

Signups: first come first serve!

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## DC - Saturday - 10:00-11:15 PDT

---

**Title:** Brazil Redux: Short Circuiting Tech-Enabled Dystopia with The Right to Repair

**When:** Saturday, Aug 13, 10:00 - 11:15 PDT

**Where:** Caesars Forum - Forum 104-105, 135-136 (Track 1)

**Speakers:** Paul Roberts, Corynne McSherry, Joe Grand, Louis Rossmann, Kyle Wiens

**SpeakerBio:** Paul Roberts , Founder, SecuRepairs.org, Editor in Chief, The Security Ledger

Paul Roberts is the publisher and Editor in Chief of The Security Ledger ([securityledger.com](http://securityledger.com)), and the founder of SecuRepairs.org, an organization of more than 200 information security professionals who support a right to repair.

**SpeakerBio:** Corynne McSherry , Legal Director, Electronic Frontier Foundation

Corynne McSherry is the Legal Director at EFF, specializing in intellectual property, open access, and free speech issues.  
Twitter: [@https://twitter.com/cmcsherr](https://twitter.com/cmcsherr)

**SpeakerBio:** Joe Grand , Founder and CEO, Grand Idea Studios

Joe Grand is a product designer, hardware hacker, and the founder of Grand Idea Studio, Inc. He specializes in creating, exploring, manipulating, and teaching about electronic devices.

Twitter: [@https://twitter.com/joegrand](https://twitter.com/joegrand)

**SpeakerBio:** Louis Rossmann , Founder, Rossmanngroup.com

Louis Rossmann is the owner of Rossmann Repair Group, a computer repair shop established in 2007 that specializes in repair of MacBooks, iPhones and other electronic devices. Louis's YouTube channel, with more than 1.7 million subscribers, documents repairs as and dispenses advice and opinions on the right to repair.

Twitter: [@https://twitter.com/rossmannsupply](https://twitter.com/rossmannsupply)

**SpeakerBio:** Kyle Wiens , CEO, iFixit

Kyle Wiens is the cofounder and CEO of iFixit, an online repair community and parts retailer internationally renowned for its open source repair manuals and product teardowns.

Twitter: [@https://twitter.com/kwiens](https://twitter.com/kwiens)

### Description:

Terry Gilliam's 1985 cult film Brazil posits a polluted, hyper-consumerist and totalitarian dystopia in which a renegade heating engineer, Archibald Tuttle, takes great risks to conduct repairs outside of the stifling and inefficient bureaucracy of "Central Services." When Tuttle's rogue repairs are detected, Central Services workers demolish and seize repaired systems under the pretext of "fixing" them. It's dark. It's also not so far off from our present reality in which device makers use always-on Internet connections, DRM and expansive copyright and IP claims to sustain "Central Services"-like monopolies on the service and repair of appliances, agricultural and medical equipment, personal electronics and more. The net effect of this

is a less- not more secure ecosystem of connected things that burdens consumers, businesses and the planet. Our panel of repair and cybersecurity experts will delve into how OEMs' anti-repair arguments trumpet cybersecurity risks, while strangling independent repair and dissembling about the abysmal state of embedded device security. We'll also examine how the emergent "right to repair" movement aims to dismantle this emerging "Brazil" style dystopia and lay the foundation for a "circular" economy that reduces waste while also ensuring better security and privacy protections for technology users.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## BHV - Saturday - 12:00-12:30 PDT

---

**Title:** Breaking the Intelligence Cycle - how to tailor intelligence function to your needs?

**When:** Saturday, Aug 13, 12:00 - 12:30 PDT

**Where:** Flamingo - Laughlin I,II,III

**SpeakerBio:** Ohad Zaidenberg

Ohad Zaidenberg is the threat intelligence strategic leader at ABInbev and the CTI League founder. Over the past ten years, Zaidenberg has focused on establishing tailor-made intelligence functions and researching adversaries and disinformation. Zaidenberg was also the lead researcher of ClearSky.

Twitter: [@https://twitter.com/ohad\\_mz](https://twitter.com/ohad_mz)

**Description:**

Threat Intelligence has become a buzzword in the last few years, and almost every organization now understands the need for intelligence to enable better protection in the organization. The intelligence function is decisive in the ability of the organization to be proactive in security, but what do we really know about establishing this function, and how can we tailor the function to our intelligence needs and our protection capabilities? In "Breaking the Intelligence Cycle", Ohad Zaidenberg, Threat Intelligence Strategic Leader and the founder of the CTI League, will review the steps that need to be taken to create this tailor-made function with considerations for the maturity level of the recipient stakeholders. Moreover, Ohad will present brand new methods for establishing PIRs and disseminating intelligence, especially for the medical sector.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## CLV - Saturday - 13:10-13:40 PDT

---

**Title:** BrokenbyDesign: Azure | Get started with hacking Azure

**When:** Saturday, Aug 13, 13:10 - 13:40 PDT

**Where:** Flamingo - Scenic Ballroom

**Speakers:** Siebren Kraak, Roy Stultiens, Ricardo Sanchez, Ricardo Sanchez

**SpeakerBio:** Siebren Kraak

Siebren Kraak is a Dutch full-stack Azure developer specializing in Security and Cloud and is currently a master's student at a university in The Netherlands.

**SpeakerBio:** Roy Stultiens

Roy Stultiens is a Security Cloud Specialist expert in serverless and containerized applications. He is a thought leader in Cloud and Kubernetes Security and is one of the larger focused cybersecurity firms in the Netherlands. He has created several other training courses on these topics.

## **SpeakerBio:**Ricardo Sanchez

Ricardo is a senior security specialist with business development and consultant background and over 10 years of experience. He exceeds in translating business needs into technical needs, and vice versa. He is currently the Lead of the Cloud Business Unit of one of the most important Cyber Security companies of the Netherlands. On top of that, he wrote two books with international distribution, has two patent applications as main inventor.

Twitter: [@https://twitter.com/ric\\_rojo](https://twitter.com/ric_rojo)

## **SpeakerBio:**Ricardo Sanchez

Ricardo Sanchez is a Senior cloud security expert with 10+ years of experience in security. He is currently leading the Cloud Security Unit in one of the larger focused cybersecurity firms in the Netherlands.

## **Description:**

Link to tool: <https://www.brokenazure.cloud/>

Because cloud and on-premise infrastructures are not alike, security analysts require a different skillset when assessing cloud infrastructure. There are multiple courses and exams that can be taken to learn how to work with and audit cloud environments. All these courses teach a global understanding of cloud security, but do not go in-depth due to all services having a different portal and setup. With this tool we will create security hacking training for the rapidly developing Azure space.

With this tool we will create security hacking training for the rapidly developing Azure space. We aim to breach the gap between theory and practice in a real secured Azure cloud environment. The software allows everyone that is trying to get into the field of cloud security to train their skills in the Azure space, with a Capture-the-Flag requiring multiple vulnerabilities that need to be exploited. All challenges are hosted online for free for anyone that wants to use the software. The challenges are beginner-friendly. The broken features are explained to give insight into why they exist and how they can be prevented. If the user is not able to figure out how to complete the challenge, additional hints (and eventually the answer) can be requested. The environment is built using the Infrastructure-As-Code language Terraform, which will all be open-source to allow other developers and security professionals to add new challenges and make the tool even better.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## **DC - Friday - 15:30-16:15 PDT**

---

**Title:** Browser-Powered Desync Attacks: A New Frontier in HTTP Request Smuggling

**When:** Friday, Aug 12, 15:30 - 16:15 PDT

**Where:** Caesars Forum - Alliance 301-309, 321 (Track 4)

## **SpeakerBio:**James Kettle , Director of Research, PortSwigger

James 'albinowax' Kettle is the Director of Research at PortSwigger - he's best known for his HTTP Desync Attacks research, which popularized HTTP Request Smuggling. James has extensive experience cultivating novel attack techniques, including web cache poisoning, HTTP/2 desync attacks, Server-Side Template Injection, and password reset poisoning. James is also the author of multiple popular open-source tools including Param Miner, Turbo Intruder, and HTTP Request Smuggler. He is a frequent speaker at numerous prestigious venues including both Black Hat USA and EU, OWASP AppSec USA and EU, and DEF CON.

Twitter: [@https://twitter.com/albinowax](https://twitter.com/albinowax)

## **Description:**

The recent rise of HTTP Request Smuggling has seen a flood of critical findings enabling near-complete compromise of numerous major websites. However, the threat has been confined to attacker-accessible systems with a reverse proxy front-end... until now.

In this session, I'll show you how to turn your victim's web browser into a desync delivery platform, shifting the request smuggling frontier by exposing single-server websites and internal networks. You'll learn how to combine cross-domain requests with server flaws to poison browser connection pools, install backdoors, and release desync worms. With these techniques I'll compromise targets including Apache, Akamai, Varnish, Amazon, and multiple web VPNs.

While some classic desync gadgets can be adapted, other scenarios force extreme innovation. To help, I'll share a battle-tested methodology combining browser features and custom open-source tooling. We'll also release free online labs to help hone your new skillset.

I'll also share the research journey, uncovering a strategy for black-box analysis that solved several long-standing desync obstacles and unveiled an extremely effective novel desync trigger. The resulting fallout will encompass client-side, server-side, and even MITM attacks; to wrap up, I'll live-demo breaking HTTPS on Apache.

---

[Return to Index](#) - Add to



- ics [Calendar](#) file

---

## ASV - Saturday - 10:00-10:25 PDT

---

**Title:** Building Your Own Satellite Ground Station

**When:** Saturday, Aug 13, 10:00 - 10:25 PDT

**Where:** Caesars Forum - Forum 112-117

**SpeakerBio:**Eric Escobar

Eric is a seasoned pentester and a Security Principal Consultant at Secureworks. 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, 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!

Twitter: [@https://twitter.com/EricEscobar](https://twitter.com/EricEscobar)

**Description:**

Are you interested in satellite communications? Would you like to help a growing community of ground station and satellite operators collect telemetry data? Well this is the talk for you. With some inexpensive hardware and a trip to your local hardware store, you too can create your very own satellite ground station. In this talk you'll learn about hardware, radio propagation and how to get started receiving data from satellites on your own ground station

---

[Return to Index](#) - Add to



- ics [Calendar](#) file

---

## IOTV - Saturday - 10:00-13:59 PDT

---

**Title:** BURP Suite, Forensics Tools & 0-day Exploit Development.

**When:** Saturday, Aug 13, 10:00 - 13:59 PDT

**Where:** Caesars Forum - Alliance 311, 320

**SpeakerBio:**Ken Pyle

## Description:

These exercises will show how simple security flaws and exposures become critical, world wide exposures in systems like the Emergency Alert System and network infrastructure from Cisco & Dell. Recreate some of the most impactful kill chains ever, learn new IOT / appsec skills, enumerate a supply chain network with a text editor, and ""live off the land"" with a few simple free tools like BURP SUITE.

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

## ASV - Friday - 09:00-16:59 PDT

**Title:** California CyberSecurity Institute Space Grand Challenge

**When:** Friday, Aug 12, 09:00 - 16:59 PDT

**Where:** Caesars Forum - Forum 112-117

## Description:

The DEF CON participants will be learning how the convergence of cybersecurity and space connect! The gamified satellite cybercrime scenario, "Mission Kolluxium Z-85-0" is ready for the next Space Captain! This is a beginner challenge. Unity based game that explores Space, Orbital Mechanics, Satellite Hacking, Deep Space Networks, Digital Forensics, Python, Wireshark, Blockchain, and Ethics! This is a great chance for a CyberNaut to learn something new!

Please register here and look for an email close to the competition day for instructions:

<https://www.cognitoforms.com/CCI17/SpaceGrandChallengeAEROSPACEVILLAGEDEFCON2022>

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

## BHV - Saturday - 16:00-16:30 PDT

**Title:** Call for Evidence: Informing the Biological Security Strategy

**When:** Saturday, Aug 13, 16:00 - 16:30 PDT

**Where:** Flamingo - Laughlin I,II,III

### **SpeakerBio:** Mariam Elgabry

Mariam Elgabry, PhD is a Cyber Fellow at Yale University Law School with a PhD in Cyber- Biosecurity from the Dawes Centre for Future Crime and the Advanced Biochemical Engineering departments at UCL. Mariam's background is in deep-tech and bioengineering, developed from leading award-winning projects in industrial settings, during her time at Astra Zeneca and Microsoft. Her work on biotechnology crime has been recognized by the UK Parliament Joint Committee for National Security and the United Nations. Mariam is founder of bronic ([www.bronic.co](http://www.bronic.co)), a security design platform for emerging technologies.

Twitter: [@https://twitter.com/MariamElgabry11](https://twitter.com/MariamElgabry11)

## Description:

Cyber-biosecurity is neither a biology-only nor a cyber-only challenge. As biotechnology continues to develop and the way that science is practiced evolves, so too does the nature of crime. In this talk, I will present a framework for mapping biotechnology crime and misuse opportunities with the aim to inform, influence and underpin evidence-based policymaking in the UK and abroad and, where relevant, to change organisational culture and practices, to improve national security.

## CPV - Saturday - 15:30-16:15 PDT

---

**Title:** Capturing Chaos: Harvesting Environmental Entropy

**When:** Saturday, Aug 13, 15:30 - 16:15 PDT

**Where:** Flamingo - Vista Ballroom

**SpeakerBio:**Carey Parker

Carey Parker is an author, podcast host, educator and retired software engineer. He is a privacy advocate whose mission is educating the masses on the basics of personal cybersecurity and the dangers of surveillance capitalism, using entertaining analogies and minimizing technical jargon.

**Description:**

Much is made for the need for strong passwords and keys, but most cryptographic processes also require a source of entropy. While computers are excellent at doing what they're told, they suck at generating true randomness. Even when gathering high quality entropy, the pool can be quickly depleted with many processes invoking cryptographic functions in rapid succession. I will discuss why entropy is so important, give examples of randomness failures, and discuss techniques for generating high quality random values in low-cost embedded systems.

---

## AVI - Saturday - 13:00-13:50 PDT

---

**Title:** CatPhish Automation - The Emerging Use of Artificial Intelligence in Social Engineering

**When:** Saturday, Aug 13, 13:00 - 13:50 PDT

**Where:** Caesars Forum - Summit 228->236

**SpeakerBio:**Justin Hutchens

No BIO available

**Description:**

Infestations of bots on social network platforms is nothing new, but the sophistication of these bots have transformed dramatically in the past few years. In the recent past, it was fairly easy for any sensible person to recognize if they were talking to a bot. But that is rapidly changing as Artificial Intelligence (AI) solutions become more advanced and more accessible. During this presentation, the speaker will explore the increasing use of AI for automated social engineering within the context of social networks, and will show how AI chat bots can be leveraged to conduct phishing attacks, compromise credentials, or distribute malware. By using emerging technologies (to include Generative Adversarial Networks for generating non-searchable profile images, and deep-learning natural language processing models for simulating human intelligence), these bots can be used to consistently fool even the most vigilant of users.

---

**Title:** Challenges in Control Validation**When:** Saturday, Aug 13, 15:00 - 15:59 PDT**Where:** Flamingo - Savoy Ballroom - BTV Main Stage**Speakers:**AJ King,Jake Williams,Kristen Cotten**SpeakerBio:**AJ King

No BIO available

**SpeakerBio:**Jake Williams

Jake Williams is the Executive Director of Cyber Threat Intelligence at SCYTHE. Williams is an IANS Faculty Member and also works as a SANS Analyst. He is a prolific speaker on topics in information security and has trained thousands of people on incident response, red team operations, reverse engineering, cyber threat intelligence, and other information security topics. Jake is the two time winner of the DC3 Digital Forensics Challenge, a recipient of the DoD Exceptional Civilian Service Award, and is one of only a handful of people to ever be certified as Master Network Exploitation Operator by the US Government.

**SpeakerBio:**Kristen Cotten

Kristen is a Cyber Threat Intelligence Analyst at SCYTHE. Prior to joining the herd she worked for the United States Department of the Army in various roles ranging from network and system administration to vulnerability management and cyber compliance. She has a penchant for solving technical puzzles, leaping from perfectly good airplanes (or cliffs), and finding the best local hole-in-the-wall restaurants. If you want to talk about foreign travel, sports nutrition, or why Episodes 4-6 are the only Star Wars movies that matter, she's your girl!

## Description:

Sample panel questions may include:

How is control validation different from red teaming? Isn't control validation just purple teaming? (it's not) How do you recommend my organization starts its first control validation exercise? What's your #1 recommendation for maturing a control validation program? What are methods for scaling control validation programs? How much validation is too much? When is the cost no longer justified?

Testing security controls is hard. Really hard. Every incident responder has lived with victims who are sure existing security controls should have prevented or detected the intrusion. While some organizations don't do any security control validation, those that do understand the challenges. While red team operations allow for point-in-time validation, how are organizations dealing with control validations during product updates or configuration changes? By and large the answer is "they aren't." On this panel, we'll discuss why control validation is difficult. Then we'll discuss recommendations for scaling control validation operations in practically any organization.

---

[Return to Index](#) - Add to- ics [Calendar](#) file

---

---

## SOC - Friday - 09:00-17:59 PDT

---

**Title:** Chillout Lounge - Entertainment**When:** Friday, Aug 12, 09:00 - 17:59 PDT**Where:** Caesars Forum - Forum 120-123, 129, 137**Speakers:**Rusty,s1gns0f1fe,Pie & Darren,Merin MC,Kampf,djdead**SpeakerBio:**Rusty

No BIO available

**SpeakerBio:**s1gnsofl1fe

No BIO available

**SpeakerBio:**Pie & Darren

No BIO available

**SpeakerBio:**Merin MC

No BIO available

**SpeakerBio:**Kampf

No BIO available

**SpeakerBio:**djdead

No BIO available

#### **Description:**

09:00 to 12:00 - Pie & Darren

12:00 to 13:30 - Kampf

13:30 to 14:30 - s1gnsofl1fe

14:30 to 15:30 - Merin MC

15:30 to 16:30 - Rusty

16:30 to 18:00 - djdead

[Return to Index](#) - Add to

[Google Calendar](#)

- ics [Calendar](#) file

## **SOC - Sunday - 09:00-14:59 PDT**

**Title:** Chillout Lounge - Entertainment

**When:** Sunday, Aug 14, 09:00 - 14:59 PDT

**Where:** Caesars Forum - Forum 120-123, 129, 137

**Speakers:**Merin MC,Pie & Darren,Rusty,s1gnsofl1fe

**SpeakerBio:**Merin MC

No BIO available

**SpeakerBio:**Pie & Darren

No BIO available

**SpeakerBio:**Rusty

No BIO available

**SpeakerBio:**s1gnsofl1fe

No BIO available

#### **Description:**

09:00 to 12:00 - Pie & Darren

12:00 to 13:00 - s1gnsofl1fe

13:00 to 14:00 - Rusty  
14:00 to 15:00 - Merin MC

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## SOC - Saturday - 09:00-17:59 PDT

---

**Title:** Chillout Lounge - Entertainment

**When:** Saturday, Aug 13, 09:00 - 17:59 PDT

**Where:** Caesars Forum - Forum 120-123, 129, 137

**Speakers:**Rusty,s1gns0fl1fe,Pie & Darren,Merin MC,Kampf,djdead

**SpeakerBio:**Rusty

No BIO available

**SpeakerBio:**s1gns0fl1fe

No BIO available

**SpeakerBio:**Pie & Darren

No BIO available

**SpeakerBio:**Merin MC

No BIO available

**SpeakerBio:**Kampf

No BIO available

**SpeakerBio:**djdead

No BIO available

### Description:

09:00 to 12:00 - Pie & Darren

12:00 to 13:30 - Kampf

13:30 to 14:30 - s1gns0fl1fe

14:30 to 15:30 - Merin MC

15:30 to 16:30 - Rusty

16:30 to 18:00 - djdead

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## SOC - Thursday - 09:00-17:59 PDT

---

**Title:** Chillout Lounge - Entertainment

**When:** Thursday, Aug 11, 09:00 - 17:59 PDT

**Where:** Caesars Forum - Forum 120-123, 129, 137

**Speakers:**Rusty,s1gns0fl1fe,Pie & Darren,Merin MC,Kampf,djdead

## **SpeakerBio:**Rusty

No BIO available

## **SpeakerBio:**s1gnsofl1fe

No BIO available

## **SpeakerBio:**Pie & Darren

No BIO available

## **SpeakerBio:**Merin MC

No BIO available

## **SpeakerBio:**Kampf

No BIO available

## **SpeakerBio:**djdead

No BIO available

### **Description:**

09:00 to 12:00 - Pie & Darren  
12:00 to 13:30 - Kampf  
13:30 to 14:30 - s1gnsofl1fe  
14:30 to 15:30 - Merin MC  
15:30 to 16:30 - Rusty  
16:30 to 18:00 - djdead

---

[Return to Index](#) - Add to



- ics [Calendar](#) file

---

## **DC - Saturday - 13:00-13:45 PDT**

---

**Title:** Chromebook Breakout: Escaping Jail, with your friends, using a Pico Ducky

**When:** Saturday, Aug 13, 13:00 - 13:45 PDT

**Where:** Caesars Forum - Forum 104-105, 135-136 (Track 1)

### **SpeakerBio:**Jimi Allee , CEO @ Lost Rabbit Labs

With 30 years in the Information Security industry, Jimi Allee has successfully navigated through many roles within the Infosec landscape, including Network/System/Security Engineering, Threat Intel/Risk Analysis, Offensive Security, Red/Blue/Purple Teaming as well as Research & Development. A former member of the US National Video Game Team, Jimi's passionate curiosity brings a gamer mentality to the world of Threat Research, Detection and Elimination. Jimi is currently the CEO of Lost Rabbit Labs, a Full-Spectrum Cybersecurity Services company that specializes in Collaborative Penetration Testing and Assessments.

Twitter: [@https://twitter.com/jimi2x303](https://twitter.com/jimi2x303)

### **Description:**

Learn how we used our Pico Ducky to escape Chromebook jail, rescue our friends along the way, and have some fun Living Off the Land! Leveraging a discovered (but previously disclosed) Command Injection vulnerability in the ChromeOS crosh shell, we rabbithole into the internal ChromeOS Linux system, obtain persistence across reboots, and exfiltrate user data even before Developer Mode has been enabled. Learn how to provision and utilize local services in order to perform Privilege Escalations, and also create a 'Master Key' with the Pico Ducky and custom GTFO 1-liners, in order to perform a full

## WS - Friday - 10:00-13:59 PDT

**Title:** CICD security: A new eldorado

**When:** Friday, Aug 12, 10:00 - 13:59 PDT

**Where:** Harrah's - Copper

**Speakers:** Remi Escourrou, Gauthier Sebaux, Xavier Gerondeau

**SpeakerBio:** Remi Escourrou , Red Team Lead

Rémi Escourrou (@remiescourrou) is leading the Red Team at Wavestone. Before moving to red team operation and exploiting CI/CD pipeline, he was involved in audits and pentests of large enterprise networks with emphasis on Active Directory. During his research time, he enjoys tackling technical problems to compromise its targets. He's passionate about the security field and already teaches workshops at BSides Las Vegas, Brucon, BSides Lisbon.

Twitter: [@https://twitter.com/remiescourrou](https://twitter.com/remiescourrou)

**SpeakerBio:** Gauthier Sebaux , Penetration Tester

Gauthier Sebaux has been performing penetration tests in Wavestone for years for a large number of clients. His passion for cybersecurity started even before he was already exploiting buffer overflows and participating to CTF competitions when he was in high school. When he is not pentesting, he administrates his personal infrastructure and contributes to open-source projects. It provided him with deep knowledge on Linux environments, Linux container isolation and more recently Kubernetes. He brought back his expertise in his work and specialized in penetration testing of DevOps infrastructure.

**SpeakerBio:** Xavier Gerondeau , Penetration Tester

Xavier Gerondeau is a penetration tester in Wavestone. He once performed a test on a CI/CD pipeline and rocked it. Because of this so-cool-ness, he became a DevOps expert in Wavestone and pwned every CI/CD pipeline he encountered during his missions. He's so talented that his clients now fear him!

### Description:

CI/CD pipelines are increasingly becoming part of the standard infrastructure within dev teams and with the rise of solutions such as Infrastructure as Code, the sensitivity level of such pipelines is escalating. In case of compromise, it is not just the applications that are at risk but the underlying systems themselves and sometimes the whole information systems. Attackers are beginning to exploit those weaknesses both for supply chain attacks but also to escalate their privileges within the victim IS.

Welcome to DataLeek company, after several decades of V-cycle development we have now decided to adopt the "agile" methodology. To do so, our IT teams have set up a CI/CD pipeline that rely on the most advanced and state-of-the-art tools available on the market. However, for some reasons, our CISO seems to doubt the security level of this brand new infrastructure and insist to perform a pentest on it.

Your mission, should you choose to accept it, is to evaluate the security level of this CI/CD pipeline and offer solutions to fix the issues identified.

In this fully hands-on workshop, we'll guide you through multiple vulnerabilities that we witnessed during numerous penetration tests. You'll learn how to:

- Get a foothold within a CI/CD pipeline
- Find interesting secrets and other information within code repositories
- How to pivot and exploit weak configuration on the orchestrator

- Compromise building nodes in order to add backdoors to artifacts
- Pivot on cloud infrastructure
- Escape Kubernetes thanks to common misconfiguration
- Perform a privilege escalation in AWS

Hand-on exercises will be performed on our lab environment with a wide variety of tools. For each attack, we will also focus on prevention, mitigation techniques and potential way to detect exploitations.

#### Materials

All attendees will need to bring a laptop capable of running virtual machines (8GB of RAM is a minimum) and an up-to-date RDP client.

#### Prereq

This training is aimed at security professionals or developers willing to understand the risks of a poorly secured CI/CD pipeline.

---

[Return to Index](#) - Add to



- ics [Calendar](#) file

---

## CLV - Sunday - 12:50-13:30 PDT

---

**Title:** Cloud Defaults are Easy Not Secure

**When:** Sunday, Aug 14, 12:50 - 13:30 PDT

**Where:** Flamingo - Scenic Ballroom

#### SpeakerBio:Igal Flegmann

Igal started his career in Microsoft's Azure Security team creating and managing identity services for Azure's secure production tenants. After a successful career in Azure Security, Igal transferred teams to work in Azure's ASCII (Azure Special Capabilities, Infrastructure, and Innovation) team, where he used his identity and security expertise to design and create security services to protect the critical infrastructure devices of the world.

To follow passion for identity and security, Igal decided to leave Microsoft and Co-found Keytos, a security company with the mission of eliminating passwords by creating easy to use PKI offerings.

Twitter: [@https://twitter.com/igal\\_fs](https://twitter.com/igal_fs)

#### Description:

In the last decade, the major cloud companies have been fighting to get market share by offering the easiest to use cloud with most services. Allowing you get a simple site up and running in a few minutes and quickly being able to scale it. While cloud providers market themselves as the most secure infrastructure for your code, their defaults are far from secure. With certificates being able to be issued without proof of domain ownership, insecure SSH by default, default passwords, and more the move to the cloud is making it easier for you and your attackers to get into your infrastructure. In this talk we will talk about common Azure errors that will get you in trouble.

---

[Return to Index](#) - Add to



- ics [Calendar](#) file

---

## CLV - Sunday - 11:20-11:50 PDT

---

**Title:** Cloud Sandboxes for Security Research - Fire from the Heavens

**When:** Sunday, Aug 14, 11:20 - 11:50 PDT

**Where:** Flamingo - Scenic Ballroom

### **SpeakerBio:**Louis Barrett

Louis L. Barrett is a Fullstack Security Researcher who has 10 years of experience in detection and response. He currently works as lead product security engineer for a SaaS AI company, where he is responsible for securing ML infrastructure and building paved road solutions for developers. He has a passion for solving hard, technical problems and integrating new software trends into traditional security practices.

Twitter: [@https://twitter.com/0daysimpson](https://twitter.com/0daysimpson)

### **Description:**

Analyzing malicious digital content safely typically requires specialized tools in a sandboxed environment, and an awareness of the risk associated with specific analysis techniques.

Traditionally the process of provisioning these environments was labor intensive, and technically demanding. In this presentation I'll show you how to use DevSecOps best practices to provision lightweight, anonymous, cloud sandboxes in seconds.

Comments: Text HOW or SHELL to 1337-561-1337\* for an early demo of what I'm presenting.

<https://github.com/shell-company/public-shell-company>

---

[Return to Index](#) - Add to



- ics [Calendar](#) file

---

## **SKY - Friday - 14:55-15:45 PDT**

---

**Title:** Cloud Threat Actors: No longer cryptojacking for fun and profit

**When:** Friday, Aug 12, 14:55 - 15:45 PDT

**Where:** LINQ - BLOQ

### **SpeakerBio:**Nathaniel Quist

Nathaniel Quist is a Principal Researcher working with Palo Alto Networks Unit 42 and Prisma Cloud teams on researching the threats facing public cloud platforms, tools, and services. He is actively focused on identifying the threats, malware and threat actor groups that target cloud environments.

Nathaniel has worked within Government, Public, and Private sectors and holds a Master of Science in Information Security Engineering (MSISE) from The SANS Institute, where he focused on Network and System Forensics, Malware Reversal, and Incident Response. He is the author of multiple blogs, reports, and whitepapers published by Palo Alto Networks' Unit 42 and Prisma Cloud as well as the SANS InfoSec Reading Room.

Twitter: [@https://twitter.com/qcueque](https://twitter.com/qcueque)

### **Description:**

Threat actors have elevated their attacks against cloud environments through the direct targeting and usage of Identity and Access Management (IAM) resources. Successful attacks not only expose the wider customer cloud environment workloads but also expose a defender's inability to successfully track the total scope of the incident using only a single cloud visibility tool. I have been tracking the evolution of cloud targeted threats and the threat actors behind them, what I have found is that actors who target cloud environments have begun to use techniques that are solely unique to cloud environments. So much so, that the Unit 42 threat intelligence team and I found it necessary to define these actors as Cloud Threat Actors. ""An individual or group posing a threat to organizations through directed and sustained access to cloud platform resources, services or embedded metadata.""

In this talk, we will guide the audience through the first-ever Cloud Threat Actor Index detailing the targeting cloud environments, who are behind these attacks, how they are targeting and leveraging techniques unique to cloud environments, and most importantly how poorly defined IAM identities open the biggest holes. We will also give the audience the knowledge needed to properly harden their cloud environments by illustrating how the most successful cloud-targeted attacks have occurred. IAM is the first line of defense in your cloud, knowing how attackers target and leverage IAM resources to evade detection is the best tool we have to properly defend your entire cloud infrastructure.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## CLV - Sunday - 13:30-13:45 PDT

---

**Title:** Cloud Village Closing Note

**When:** Sunday, Aug 14, 13:30 - 13:45 PDT

**Where:** Flamingo - Scenic Ballroom

**SpeakerBio:**Jayesh Singh Chauhan

No BIO available

**Description:**No Description available

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## CLV - Friday - 10:00-10:10 PDT

---

**Title:** Cloud Village Opening Note

**When:** Friday, Aug 12, 10:00 - 10:10 PDT

**Where:** Flamingo - Scenic Ballroom

**SpeakerBio:**Jayesh Singh Chauhan

No BIO available

**Description:**No Description available

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## MIV - Saturday - 12:30-13:45 PDT

---

**Title:** Cognitive Security in Theory and Practice

**When:** Saturday, Aug 13, 12:30 - 13:45 PDT

**Where:** Caesars Forum - Summit 221->236

**SpeakerBio:**Sara-Jayne Terp

SJ Terp applies information security practices to defend against disinformation and other online harms, including extremism. She has run large incident responses, set up response systems for election- and health-based cognitive security around the

world, advises companies on disinformation risk management, and has built a body of research and tools for running and operating cognitive security operations centres, including the DISARM (formerly AMITT) frameworks for rapidly sharing disinformation data. She teaches cybersecurity and cognitive security at the University of Maryland.

### Description:

No Description available

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## MIV - Friday - 11:30-13:30 PDT

---

**Title:** Cognitive Security: Human Vulnerabilities, Exploits, & TTPs

**When:** Friday, Aug 12, 11:30 - 13:30 PDT

**Where:** Caesars Forum - Summit 221->236

### SpeakerBio:

Matthew Canham

Dr. Matthew Canham is the CEO of Beyond Layer Seven, a company dedicated to understanding and addressing the human element in cybersecurity. In addition to his primary role, Dr. Canham is also an affiliated faculty member at George Mason University where his research focuses on human susceptibility to mis-dis-mal (MDM) information operations and remote online social engineering attacks. He holds a PhD in Cognitive Neuroscience from the University of California at Santa Barbara, and he is a certified digital forensics examiner and mobile device security analyst.

### Description:

No Description available

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## SKY - Friday - 09:30-10:20 PDT

---

**Title:** Combatting sexual abuse with threat intelligence techniques

**When:** Friday, Aug 12, 09:30 - 10:20 PDT

**Where:** LINQ - BLOQ

### SpeakerBio:

Aaron DeVera

Aaron DeVera is a New York-based security researcher whose experience spans from the takedown of multi-million dollar criminal botnets to threat intelligence operations for global financial services companies. They are a member of the New York Cyber Sexual Abuse Taskforce, a founding member of the Cabal hacker collective, and a founder of Backchannel, which builds tools for adversary intelligence and adversary attribution. Their previous speaking engagements include SXSW, Botconf, SummerCon, The Diana Initiative, and within the information security community.

Twitter: [@https://twitter.com/aaronsdevera](https://twitter.com/aaronsdevera)

### Description:

The techniques and tactics used against cyber adversaries can be effective against perpetrators of sexual violence. Join the representatives from the Cabal hacker collective as they chart their success in attributing online behavior, creating intelligence pipelines, and survivor outreach in the wake of the growing threat of cyber sexual abuse. The featured case studies are real-life scenarios where familiar infosec operations ended up making a huge impact in cases against cyberstalkers, sex criminals, and hackers.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

## **SKY - Saturday - 17:05-17:55 PDT**

---

**Title:** Coming Home to Def Con: A Deep Dive into the Real Essence and Ethos of Hacking

**When:** Saturday, Aug 13, 17:05 - 17:55 PDT

**Where:** LINQ - BLOQ

**SpeakerBio:**Richard Thieme , ThiemeWorks

Richard Thieme is an author/professional speaker who addresses “the human in the machine,” technology-related security and intelligence issues as they come home to our humanity. He has published hundreds of articles, dozens of stories, seven books, and delivered hundreds of speeches, including for NSA, FBI, the Secret Service, etc. He spoke in 2021 at Def Con for the 25th year and has keynoted security conferences in 15 countries. His latest book about an intelligence professional, "Mobius: A Memoir," is a novel receiving over-the-top reviews.

Twitter: [@https://twitter.com/neuralcowboy](https://twitter.com/neuralcowboy)

### **Description:**

Coming home to Def Con is more than a metaphor. I said a quarter century ago when I first spoke here that this was our psychic home and where we knew we belonged. This talk spells out the deeper, most compelling , and most poignant reasons for why that's true. I have explored the traumatic impacts of the dark side of our work and the triumphant discovery of real community and you can't have one without the other. This talk is a deep dive into the dynamics of both hacking and this particular con and why we love both.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## **DC - Friday - 10:00-10:20 PDT**

---

**Title:** Computer Hacks in the Russia-Ukraine War

**When:** Friday, Aug 12, 10:00 - 10:20 PDT

**Where:** Caesars Forum - Alliance 301-309, 321 (Track 4)

**SpeakerBio:**Kenneth Geers , Very Good Security / NATO Cyber Centre / Atlantic Council

Dr. Kenneth Geers works at Very Good Security. He is an Atlantic Council Cyber Statecraft Initiative Senior Fellow, a NATO Cooperative Cyber Defence Centre of Excellence Ambassador, and a Digital Society Institute-Berlin Affiliate. Kenneth served for twenty years in the US Government: in the Army, National Security Agency (NSA), Naval Criminal Investigative Service (NCIS), and NATO. He was a professor at the Taras Shevchenko National University of Kyiv in Ukraine from 2014-2017. He is the author of "Strategic Cyber Security", editor of "Cyber War in Perspective: Russian Aggression Against Ukraine", editor of "The Virtual Battlefield", and technical expert to the "Tallinn Manual".

Twitter: [@https://twitter.com/KennethGeers](https://twitter.com/KennethGeers)

### **Description:**

The Russia-Ukraine war has seen a lot of computer hacking, on both sides, by nations, haxor collectives, and random citizens, to steal, deny, alter, destroy, and amplify information. Satellite comms have gone down. Railway traffic has been stymied. Doxing is a weapon. Fake personas and false flags are expected. Every major platform has had issues with confidentiality, integrity, and availability. Hacked social media and TV have been a hall of mirrors and PSYOP. Russian comms are unreliable, so Ukrainian nets have become honeypots. Hackers have been shot in the kneecaps. Talking heads have called for a RUNET shutdown. The Ukrainian government has appealed for hacker volunteers – just send your expertise, experience, and a reference. The Great Powers are hacking from afar, while defending their own critical infrastructure, including nuclear command-and-control. Ukraine has many hacker allies, while Russian hackers are fleeing their country in record numbers. Some lessons so far: connectivity is stronger than we thought, info ops are stealing the day, drones are the future, and it is

always time for the next hack.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## SKY - Saturday - 09:30-10:20 PDT

---

**Title:** Confessions of a CISO

**When:** Saturday, Aug 13, 09:30 - 10:20 PDT

**Where:** LINQ - BLOQ

**SpeakerBio:**Laura Whitt-Winyard

Laura Whitt-Winyard is the CISO of Malwarebytes. Whitt-Whinyard has achieved distinction as a Fellow at the Institute for Critical Infrastructure Technology. As a Fellow, she contributed to the Cyberspace Solarium Commission's report on cybersecurity plus The Cybershield Act S.965 of the 117th Congress. She is also an International Advisory Board Member and Women in Technology board member at HMG Strategy.

With a unique and wide-ranging track record of executive leadership spanning more than two decades in the cybersecurity industry, Whitt-Winyard is among the foremost security leaders in her field today. She brings with her a deeply technical background rooted in her past experience as a security engineer, which in turn has helps to drive immediate progress.

Twitter: [@https://twitter.com/L\\_WhittWinyard](https://twitter.com/L_WhittWinyard)

**Description:**

Ever thought of becoming a CISO? Want to know the ugly truth of security from the top down?

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## PLV - Saturday - 14:00-15:45 PDT

---

**Title:** Confronting Reality in Cyberspace: Foreign Policy for a Fragmented Internet

**When:** Saturday, Aug 13, 14:00 - 15:45 PDT

**Where:** Caesars Forum - Summit 224-225 - Policy Collaboratorium

**Speakers:**Neal Pollard,Jason Healey

**SpeakerBio:**Neal Pollard , Ernst & Young

No BIO available

**SpeakerBio:**Jason Healey , Senior Research Scholar at Columbia University SIPA

No BIO available

**Description:**

The global internet is in large part a creation of the United States. The internet's basic structure—a reliance on the private sector and the technical community, relatively light regulatory oversight, and the protection of speech and the promotion of the free flow of information—reflected American values. Moreover, U.S. strategic, economic, political, and foreign policy interests were served by the global, open internet. But the United States now confronts a starkly different reality. The utopian vision of an open, reliable, and secure global network has not been achieved and is unlikely ever to be realized. Today, the internet is less free, more fragmented, and less secure.

The United States needs a new strategy that responds to what is now a fragmented and dangerous internet. The Council on Foreign Relations launched an independent task force to develop findings and recommendations for a new foreign policy for cyberspace. This session will seek input from the DEF CON community on specific foreign policy measures, to help guide Washington's adaptation to today's more complex, variegated, and dangerous cyber realm.

Come prepared to discuss topics, such as: Developing a digital privacy policy that is interoperable with Europe's General Data Protection Regulation (GDPR); Building a coalition for open-source software; Developing coalition-wide practices for the Vulnerabilities Equities Process (VEP); Clean up U.S. cyberspace by offering incentives for internet service providers (ISPs) and cloud providers to reduce malicious activity within their infrastructure.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## DC - Sunday - 14:00-15:15 PDT

---

**Title:** Contest Closing Ceremonies & Awards

**When:** Sunday, Aug 14, 14:00 - 15:15 PDT

**Where:** Caesars Forum - Academy 401-410, 421 (Track 3)

**SpeakerBio:** Grifter , DEF CON, Contests & Events

No BIO available

### Description:

DEF CON Contests & Events Awards, come find out who won what!!

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## ASV - Sunday - 10:30-11:20 PDT

---

**Title:** Control Acquisition Attack of Aerospace Systems by False Data Injection

**When:** Sunday, Aug 14, 10:30 - 11:20 PDT

**Where:** Caesars Forum - Forum 112-117

**SpeakerBio:** Garrett Jares

Garrett Jares is a Ph.D. student in the Department of Aerospace Engineering at Texas A&M University and a 2020 Recipient of the NSF Graduate Research Fellowship. His doctoral dissertation investigates cyber-attacks designed to take control of an aircraft by targeting the vehicle's sensor data

### Description:

The most dangerous cyber threat faced by unmanned air systems and other autonomous vehicles is the threat of hijacking via cyberattack. This work investigates and develops a novel method of attack by false data injection of the vehicle's measurement data. It is shown that this approach is system agnostic and can be used to take over a system without any prior knowledge of the system. The attack is demonstrated in both simulation and hardware experiments.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## **DL - Saturday - 14:00-15:55 PDT**

---

**Title:** Control Validation Compass – Threat Modeling Aide & Purple Team Content Repo

**When:** Saturday, Aug 13, 14:00 - 15:55 PDT

**Where:** Caesars Forum - Caucus Boardroom

### **SpeakerBio:**Scott Small

Scott Small has over 10 years' professional experience as a security & intelligence practitioner. Currently an analyst at a major retailer, Scott's prior roles focused on advising security teams across maturity levels on technical and strategic applications of intelligence. Scott is an active member of the professional security & intelligence communities. In addition to speaking and contributing to community projects, he has launched two projects that aggregate and streamline publicly accessible intelligence/security resources, as well as authored his own original tools & resources.

### **Description:**

Control Validation Compass ("Control Compass") provides a needed public resource that enables cyber security teams to actually operationalize MITRE ATT&CK for its best purpose: prioritized control validation. Control Compass unites tens of thousands of detection rules, offensive security scripts, and policy recommendations from 60+ open sources – all aligned with MITRE ATT&CK – into the largest single, continuously updated reference library for such content, wrapped in an easily searchable interface. This saves defenders, red teamers, and intel & GRC analysts serious time & effort when researching content for purple teaming efforts (aka control validation). Like its input components and sources, Control Compass resource sets are openly available to all, no strings attached. Control Compass supports a powerful second use case informed by its author's experience advising security & intelligence teams across maturity levels: the tool also provides a library of unique, openly available threat landscape summaries organized by key adversary categories, including motivation, location, and victim industry. By enabling easy identification of relevant threat intelligence – and a simple UI-based workflow to instantly surface corresponding security controls – Control Compass greatly lowers the barrier to building accurate, intelligence-driven threat models and helps drive tighter control validation feedback loops around the threats that matter most to a given organization.

Audience: Intelligence analysts, SOC/blue team/defenders, red team/adversary emulation, GRC analysts

---

[Return to Index](#) - Add to [!\[\]\(62c0cd5d58db9a9a04d294142dfb6294\_img.jpg\) Google Calendar](#) - ics [Calendar](#) file

---

## **WS - Saturday - 15:00-18:59 PDT**

---

**Title:** Creating and uncovering malicious containers.

**When:** Saturday, Aug 13, 15:00 - 18:59 PDT

**Where:** Harrah's - Elko

**Speakers:**Adrian Wood,Griffin Francis,David Mitchell

### **SpeakerBio:**Adrian Wood , Security Researcher

Adrian Wood, aka threlfall, discovered a love for hacking from cracking and modding video games and from the encouragement of online friends. He has worked as a red team consultant for WHITEHACK, a company he founded, and later as a lead engineer for an offensive research team at a US bank, where he was very interested in appsec, container security, CI/CD security and also founded their bug bounty program. He currently works for Dropbox, working on application security. In his free time, he enjoys playing saxophone, working on vintage cars, and fly-fishing.

### **SpeakerBio:**Griffin Francis , Security Research Consultant

Griffin Francis (@aussinfosec) is a lead information security research consultant at Wells Fargo. Previously having worked at Trustwave in Sydney, Australia. His interests are within Web Application security and Bug Bounty. His research has identified vulnerabilities in companies and organisations including Apple, Microsoft, Mozilla, Oracle, Riot Games & AT&T.

When not at the computer, Griffin can be found attending music festivals and travelling.

Twitter: [@https://twitter.com/aussinfosec](https://twitter.com/aussinfosec)

## **SpeakerBio:**David Mitchell , Red Team

David Mitchell, aka digish0, started his hacking career as a script kiddie running 7th Sphere in mIRC in high school. Later falling in with some Linux/RedHat nerds at a local 2600 group at college while studying CS, etc. He got into Linux, started an IT career, later rediscovering his hacking script kiddie roots when a local hacker space opened up and shared members with a lockpicking group that worked in infosec as penetration testers, etc where he discovered he could get paid to do the things he liked doing in high school/college. He now works professionally as a red team member and cyber security researcher at a large financial institution. The rest of the time he spends being a dad/husband, trying not to get injured in Muay Thai/BJJ or mountain biking, and listening to either very expensive or very cheap vinyl.

## **Description:**

Containers are the future. Like it or not even the most technically conservative industries are shifting to them. What that means for the bad actors is they get access to an excellent delivery mechanism for malware deployment in organizations, offering a wide variety of detection avoidance and persistence mechanisms. Fear not protectors, containers also offer ways to detect these, but can be fraught with challenges. Whether you're red, blue or just container curious this workshop is for you.

In this workshop, you will get hands-on with containers and kubernetes, - starting with introductory content - learning how they work, where and how to hide or find things, how to identify indicators of compromise, indicators of attack, and how to apply analysis to gain a deeper understanding of container malware and what is going on inside containers.

This workshop will utilize the Google Cloud Platform alongside command line operands and a small amount of open source tooling to learn both offensive and defense techniques on containers. By the end, you'll have a solid mental model of how containers work, how they are managed and deployed, and be equipped with the ability to analyze container images, identify problems, and identify familiar patterns. Ultimately, these skills will allow you to generate valuable insights for your organization's defense or aid you in your next attack.

This is a fast-paced course designed to take you deep into the world of containers, making tooling like Kubernetes much more intuitive and easy to understand. Labs will be used to reinforce your learnings, and the course comes with very detailed notes and instructions for setup which you can repeat on your own time. This course will provide references to scripts that make certain tasks easier, but we will be challenging you to learn the process and reasoning behind them rather than relying on automation.

Attendees will be provided with all the lab material used in the course in digital format, including labs, guides and virtual machine setup.

### Materials

A Google Cloud free tier account (basically a fresh gmail account), and an internet connected computer. We hope to send out instructions to attendees prior to the class, so they can be ready on the day.

### Prereq

None, the class is well designed to allow those with little to no linux, kubernetes or cloud familiarity to follow along, but a basic familiarity with Linux and terminal will allow attendees to focus on the work.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## **BICV - Friday - 11:00-11:59 PDT**

---

**Title:** Creating More Black Hackers: Growth Systems for Cybersecurity Enthusiasts

**When:** Friday, Aug 12, 11:00 - 11:59 PDT

**Where:** Virtual - BIC Village

**SpeakerBio:**Segun Ebenezer Olaniyan  
No BIO available

**Description:**No Description available

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## DC - Saturday - 17:30-18:15 PDT

---

**Title:** Crossing the KASM -- a webapp pentest story

**When:** Saturday, Aug 13, 17:30 - 18:15 PDT

**Where:** Caesars Forum - Forum 106-110, 138-139 (Track 2)

**Speakers:**Justin Gardner, Samuel Erb

**SpeakerBio:**Justin Gardner , Full-time Bug Bounty Hunter

Justin Gardner is a full-time bug bounty hunter who spent the last two years traveling around Japan with his wife Mariah, and is currently in the process of settling back down in Richmond, VA to adopt some kids and start a family. His expertise lies mostly in Web Hacking with a bug bounty focus, but he also has experience with Ethereum Smart Contract Auditing, Penetration Testing, and Mobile App Hacking. He hopes to pivot into binary exploitation over the next couple years as well.  
Twitter: [@https://www.twitter.com/Rhynorater](https://www.twitter.com/Rhynorater)

**SpeakerBio:**Samuel Erb , Hacker

Samuel Erb is a 2x black badge winner with Co9 in the Badge Challenge and is working to make the Internet a safer place. He has also presented 3x previously at the Packet Hacking Village. Outside of hacking, you will likely find Sam in a climbing gym or on the side of a mountain.

Twitter: [@https://twitter.com/erbbysam](https://twitter.com/erbbysam)

### Description:

In this talk we will tell the story of an insane exploit we used to compromise the otherwise secure KASM Workspaces software. KASM Workspaces is enterprise software for streaming virtual workstations to end users built on top of Docker.

This talk will span python binary RE, header smuggling, configuration injection, docker networking and questionable RFC interpretation. We hope to show you a little bit of what worked and a lot a bit of what didn't work on our quest to exploit this heisenbug.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## CPV - Saturday - 13:00-13:45 PDT

---

**Title:** Cryptle: a secure multi-party Wordle clone with Enarx

**When:** Saturday, Aug 13, 13:00 - 13:45 PDT

**Where:** Flamingo - Vista Ballroom

**Speakers:**Tom Dohrmann, Richard Zak, Nick Vidal

**SpeakerBio:**Tom Dohrmann

Rust enthusiast and contributor to several open source projects, including the Enarx project.

## **SpeakerBio:**Richard Zak

After a decade of malware and machine learning research, and publishing several papers, Richard decided to switch gears and work on Enarx and Confidential Computing. He is also a part-time computer science instructor at a university. Outside of work, he enjoys working on open source projects, playing video games, and tinkering with various technologies. Website: <https://rjzak.github.io/>

## **SpeakerBio:**Nick Vidal

Nick Vidal is the Community Manager of Profian and the Enarx project, which is part of the Confidential Computing Consortium from the Linux Foundation. Previously, he was the Director of Community and Business Development at the Open Source Initiative, Director of Americas at the Open Invention Network, and one of the community leaders of the Drupal project in Latin America

## **Description:**

Wordle is a popular web-based game, where a single player has to guess a five-letter word in six attempts, with yellow/green colored tiles shown as hints in each round, indicating letters that match with the secret word.

We've created an open source clone of Wordle called Cryptle, with the goal of demonstrating data encryption in use, where the processing of the data is done in a Trusted Execution Environment (TEE), and only accessible to the Cryptle application.

Cryptle is similar to Wordle but one important difference is that it is multi-party and the secret words are suggested by the players themselves. Each player proposes words that are most likely to match those sent by others. The words are sent to the Cryptle application deployed and running in an Enarx Keep (a specific TEE instance) and are only revealed to the players when there's a match between the secret words.

The standard way to engage with the game is for players to guess the secret words by playing Cryptle from the client side. However, we will also be allowing an alternative: players may write an open source application which runs with root privileges on the host side and attempts to derive or otherwise guess the secret words. Since Cryptle makes use of Confidential Computing, players shouldn't be able to read what's in memory, even with root access.

We'll provide an overview of an exploit of Enarx and we'll explain how we were able to fix it. Attendees will be invited to find new vulnerabilities as part of the Cryptle Hack Challenge.

---

[Return to Index](#) - Add to



- ics [Calendar file](#)

---

## **BICV - Saturday - 11:00-11:45 PDT**

---

**Title:** Cryptocurrency: A Bridge Across the Digital Divide

**When:** Saturday, Aug 13, 11:00 - 11:45 PDT

**Where:** Virtual - BIC Village

## **SpeakerBio:**Stephanie Barnes

No BIO available

**Description:**No Description available

---

[Return to Index](#) - Add to



- ics [Calendar file](#)

---

**Title:** Cryptosploit

**When:** Sunday, Aug 14, 13:30 - 14:15 PDT

**Where:** Flamingo - Vista Ballroom

**Speakers:**Matt Cheung,Benjamin Hendel

**SpeakerBio:**Matt Cheung , Hacker

Matt Cheung started developing his interest in cryptography during an internship in 2011. He worked on implementation of a secure multi-party protocol by adding elliptic curve support to an existing secure text pattern matching protocol.

Implementation weaknesses were not a priority and this concerned Matt. This concern prompted him to learn about cryptographic attacks from Dan Boneh's crypto 1 course offered on Coursera and the Matasano/cryptopals challenges. From this experience he has given workshops at the Boston Application Security Conference, BSidesLV, DEF CON, and the Crypto and Privacy Village.

**SpeakerBio:**Benjamin Hendel

<br>

**Description:**

Cryptosploit is a new tool intended to aid in the development and use of cryptographic attacks in a variety of scenarios. Inspired by the cryptopals challenges and tools like metasploit this talk will discuss the origin of this tool and its uses. The main innovation of this tool is to write modules to implement attacks and separate code to interact with cryptographic systems called oracles. In this talk we will discuss how the attacks work and demonstrate how to execute them with this tool. The hope is this tool will encourage the use of cryptographic attacks where applicable by lowering the barrier of entry and community development.

---

[Return to Index](#) - Add to



- ics [Calendar](#) file

---

## WS - Saturday - 10:00-13:59 PDT

---

**Title:** CTF 101: Breaking into CTFs (or “The Petting Zoo” - Breaking into CTFs)

**When:** Saturday, Aug 13, 10:00 - 13:59 PDT

**Where:** Harrah's - Silver

**Speakers:**Robert Fitzpatrick,Chris Forte

**SpeakerBio:**Robert Fitzpatrick

Robert Fitzpatrick is a military veteran of over 19 years. He began his cyber life leading the Information Assurance office, and quickly moved up to run the Network Operations Center, as well as the Network Test and Evaluation center. He has built multiple operations centers in both homeland and austere locations, purchased satellite infrastructures, and led vulnerability investigations for classified networks. He is also a co-founder of DC702 and enjoys training new students on an eclectic array of subjects surrounding his interests.

**SpeakerBio:**Chris Forte , Security Researcher

Christopher Forte is a security researcher, technology enthusiast, and cybersecurity professional. With experience ranging from software development to physical red teaming, he is passionate about keeping security and various forms of engineering at the center of his focus. Christopher leads his local TOOOL chapter and is a co-founder of the DC702 group.

Twitter: [@https://twitter.com/chris\\_forte](https://twitter.com/chris_forte)

**Description:**

Breaking into the capture the flag (CTF) world can be daunting. With much of the world going virtual, many companies,

organizations, and individuals are sponsoring capture the flag competitions and people are using these types of events, or various hacking platforms (e.g., Offensive Security's Proving Grounds or Hack The Box), to learn and practice new skills. Unfortunately, many feel overwhelmed when faced with these challenges or don't know where to start. This workshop will introduce the basics of CTFs and provide resources, tips, and fundamental skills that can be helpful when getting started.

This workshop will start with an overview of the CTF landscape, why we do them, and what value they have in the scope of the hacking community. This workshop will include various resources, a couple walkthroughs to show how to approach CTFs, and how it may differ from "real world" hacking challenges. Next, a short CTF will be hosted to give attendees hands-on experience solving challenges while being able to ask for help to successfully navigate the challenges. By the end of the workshop, the group will have worked through various types of CTF challenges, and have the confidence to participate in other CTFs hosted throughout the year.

Areas of focus will include:

- \* Common platforms and formats
- \* Overview of online resources
- \* Common tools used in CTFs and hacking challenges
- \* Basics of web challenges
- \* Basics of binary exploitation and reversing challenges
- \* Basics of cryptographic challenges
- \* Basics of forensic and network traffic challenges
- \* Some ways of preparing for your next CTF / Hacking challenge

#### Materials

Laptop Debian-based Virtual Machine (e.g., Kali) is recommended, and USB install drives will be available. Virtualized environment or Kali is not required but Kali will provide all the tools useful in solving the challenges and help standardize available tools. All challenge solutions will be possible using default Kali installations.

#### Prereq

Be curious about CTFs and have a very basic knowledge of or exposure to fundamental topics (e.g., Linux, websites, networking, data encoding and encryption) Exposure to the above concepts will help during the workshop defined CTF challenges but is not required for the workshop

---

[Return to Index](#) - Add to [!\[\]\(4550fa408728621e1512e09426946f1b\_img.jpg\) Google Calendar](#) - ics [Calendar](#) file

---

## PT - Tuesday - 09:00-16:59 PDT

---

**Title:** Customizable Binary Analysis: Using angr to its full potential

**When:** Tuesday, Aug 16, 09:00 - 16:59 PDT

**Where:** Caesars Forum

**Speakers:** Audrey Dutcher, Fish Wang

#### **SpeakerBio:** Audrey Dutcher

Audrey is a PhD student at Arizona State university. She loves reverse engineering, fruit, Celeste (2018), Python, Rust, and symbolic execution.

Twitter: [@https://twitter.com/rhelmot](https://twitter.com/rhelmot)

#### **SpeakerBio:** Fish Wang

Fish Wang is an Assistant Professor at Arizona State University. He is extremely interested in demystifying all sorts of binary code, and his main research interests are software vulnerability discovery, automated exploit generation, and binary decompilation. Fish is a co-founder and a core maintainer of angr.

Twitter: [@https://twitter.com/ltfish\\_](https://twitter.com/ltfish_)

#### **Description:**

Latest details, requirements, description, cost:

<https://defcontrainings.myshopify.com/products/fish-wang-customizable-binary-analysis-using-angr-to-its-full-potential>

## Training description:

One of the most badass skills a hacker can possess is the ability to find and pwn vulnerabilities in binary software. This is enabled by a long history of complex tools: OllyDBG, SoftICE, IDA Pro, Binary Ninja, and now: angr. Built using cutting-edge techniques straight out of research labs around the world, angr enables analysts to swiftly carry out advanced reasoning over software to understand complex code and find the juicy hidden vulnerabilities within. While angr is arguably one of the most user-friendly binary analysis frameworks available on the market, it is never an easy task to use it to its full potential, especially when facing less common architectures (such as PowerPC), niche operating environments (bare-metal binaries or embedded architectures), or unique tasks (e.g., binary code optimization, exploit generation, efficient vulnerability discovery, etc.). To assist users, especially medium-level and professional reverse engineers to effectively and efficiently use angr in their daily work, we designed this two-day course focusing on the use of non-trivial capabilities that angr offers, as well as customizing angr's advanced analyses for users' needs. This course is extremely practical and hands-on: Besides a five-hour lecture, core angr developers will guide students to solve over ten specially crafted problems with angr. This course will focus on Linux userspace binaries (x86-64 and ARM), Windows userspace binaries (x86-64), and firmware images (ARM). After completing this course, students will master practical angr skills that will help them reverse engineer userspace binary programs and assess them for defects and vulnerabilities.

---

[Return to Index](#) - Add to



- ics [Calendar](#) file

---

## PT - Monday - 09:00-16:59 PDT

---

**Title:** Customizable Binary Analysis: Using angr to its full potential

**When:** Monday, Aug 15, 09:00 - 16:59 PDT

**Where:** Caesars Forum

**Speakers:** Audrey Dutcher, Fish Wang

**SpeakerBio:** Audrey Dutcher

Audrey is a PhD student at Arizona State university. She loves reverse engineering, fruit, Celeste (2018), Python, Rust, and symbolic execution.

Twitter: [@https://twitter.com/rhelmot](https://twitter.com/rhelmot)

**SpeakerBio:** Fish Wang

Fish Wang is an Assistant Professor at Arizona State University. He is extremely interested in demystifying all sorts of binary code, and his main research interests are software vulnerability discovery, automated exploit generation, and binary decompilation. Fish is a co-founder and a core maintainer of angr.

Twitter: [@https://twitter.com/ltfish\\_](https://twitter.com/ltfish_)

## Description:

Latest details, requirements, description, cost:

<https://defcontrainings.myshopify.com/products/fish-wang-customizable-binary-analysis-using-angr-to-its-full-potential>

## Training description:

One of the most badass skills a hacker can possess is the ability to find and pwn vulnerabilities in binary software. This is enabled by a long history of complex tools: OllyDBG, SoftICE, IDA Pro, Binary Ninja, and now: angr. Built using cutting-edge techniques straight out of research labs around the world, angr enables analysts to swiftly carry out advanced reasoning over software to understand complex code and find the juicy hidden vulnerabilities within. While angr is arguably one of the most user-friendly binary analysis frameworks available on the market, it is never an easy task to use it to its full potential, especially when facing less common architectures (such as PowerPC), niche operating environments (bare-metal binaries or embedded architectures), or unique tasks (e.g., binary code optimization, exploit generation, efficient vulnerability discovery, etc.). To assist users, especially medium-level and professional reverse engineers to effectively and efficiently use

angr in their daily work, we designed this two-day course focusing on the use of non-trivial capabilities that angr offers, as well as customizing angr's advanced analyses for users' needs. This course is extremely practical and hands-on: Besides a five-hour lecture, core angr developers will guide students to solve over ten specially crafted problems with angr. This course will focus on Linux userspace binaries (x86-64 and ARM), Windows userspace binaries (x86-64), and firmware images (ARM). After completing this course, students will master practical angr skills that will help them reverse engineer userspace binary programs and assess them for defects and vulnerabilities.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## ASV - Friday - 13:00-13:25 PDT

---

**Title:** Cyber Star Card Game Tutorial

**When:** Friday, Aug 12, 13:00 - 13:25 PDT

**Where:** Caesars Forum - Forum 112-117

**SpeakerBio:** Rick White

No BIO available

### Description:

Cyber Star© is a role-play game exploring the implications of cyber security on the projection of space power. Players compete to become the predominant space power by carefully investing in space assets, ASAT weapons, and cyber capabilities both to advance their own objectives and thwart those of their opponents. No specialized knowledge or skills are required to play. This competition will consist of a practice round, main round, and finals. The winner will receive a 2022 Aerospace Village Badge!

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## ASV - Friday - 13:00-12:59 PDT

---

**Title:** Cyber Star© Competition Presented by The Space ISAC

**When:** Friday, Aug 12, 13:00 - 12:59 PDT

**Where:** Caesars Forum - Forum 112-117

### Description:

Cyber Star© is a role-play game exploring the implications of cyber security on the projection of space power. Players compete to become the predominant space power by carefully investing in space assets, ASAT weapons, and cyber capabilities both to advance their own objectives and thwart those of their opponents. No specialized knowledge or skills are required to play.

This competition will consist of a practice round, main round, and finals. The winner will receive a 2022 Aerospace Village Badge!

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

**Title:** Cyber Threats Against Aviation Systems: The Only Threat Briefing You Really Need

**When:** Saturday, Aug 13, 11:00 - 11:50 PDT

**Where:** Caesars Forum - Forum 112-117

**SpeakerBio:** Teresa Merklin , Fellow attached to the Aeronautics Cyber Range

Teresa Merklin is a Fellow attached to the Aeronautics Cyber Range at Lockheed Martin. That facility is chartered to perform highly specialized cybersecurity testing and evaluation of embedded avionics and weapons systems. She specializes in Cyber Risk Assessment across the Aeronautics portfolio.

### Description:

Developing and maintaining Aerospace systems for cyber resilient operation requires knowledge and insight into adversarial techniques and tactics. The historical origins of cyber risk assessment and cyber development standards center around an understanding of the threat actors who perpetrate attacks on Aerospace systems. This presentation cuts through the historical origins of that focus so developers and operators of aviation systems, space systems, and critical infrastructure can leverage that insight into effective adversarial targeting, capabilities required, and cyber effects that align with intent. Finally this talk describes specific actionable analysis that can help industry drive toward more cyber resilient Aerospace systems and get “Left of Boom” of adversarial cyber-attack.

---

[Return to Index](#) - Add to



- ics [Calendar](#) file

---

## DL - Friday - 14:00-15:55 PDT

---

**Title:** CyberPeace Builders

**When:** Friday, Aug 12, 14:00 - 15:55 PDT

**Where:** Caesars Forum - Accord Boardroom

**SpeakerBio:** Adrien Ogee , Chief Operations Officer

Adrien is currently Chief Operations Officer at the CyberPeace Institute, a cybersecurity non-profit based in Switzerland. At the Institute, he provides cybersecurity assistance to vulnerable communities around the world. Adrien has more than 15 years of experience in various cyber crisis response roles in the private sector, the French Cybersecurity Agency (ANSSI), the European Cybersecurity Agency (ENISA), and the World Economic Forum. Adrien holds an MEng in telecommunication and information systems, an MSc in Global Security and a Master in Business Administration.

### Description:

The CyberPeace Builders are pro hackers who volunteer to help NGOs improve their cybersecurity. Through a portal that I'll demo, hackers can access a variety of short engagements, from 1 to 4 hours, to provide targeted cybersecurity help to NGOs on topics ranging from staff awareness to DMARC implementation, password management and authentication practices, breach notification, OSINT and dark web monitoring, all the way to designing a cyber-related poster for the staff, reviewing their privacy policy and cyber insurance papers. The programme is the world's first and only skills-based volunteering opportunity for professionals in the cybersecurity industry; it has been prototyped over 2 years, was launched in July 2021 and is now being used by over 60 NGOs worldwide, ultimately helping to protect over 350 million vulnerable people and \$500 million in funds. I'll demo the platform, show the type of help NGOs need and explain how NGOs and security professionals can leverage the programme.

Audience: Security professionals, NGOs

---

[Return to Index](#) - Add to



- ics [Calendar](#) file

## DC - Saturday - 15:00-15:20 PDT

---

**Title:** Déjà Vu: Uncovering Stolen Algorithms in Commercial Products

**When:** Saturday, Aug 13, 15:00 - 15:20 PDT

**Where:** Caesars Forum - Forum 104-105, 135-136 (Track 1)

**Speakers:** Patrick Wardle, Tom McGuire

**SpeakerBio:** Patrick Wardle, Founder, Objective-See Foundation

Patrick Wardle is the creator of the non-profit Objective-See Foundation, author of the “The Art of Mac Malware” book series, and founder of the “Objective by the Sea” macOS Security conference.

Having worked at NASA and the NSA, as well as presenting at countless security conferences, he is intimately familiar with aliens, spies, and talking nerdy.

Patrick is passionate about all things related to macOS security and thus spends his days finding Apple 0days, analyzing macOS malware, and writing free open-source security tools to protect Mac users.

Twitter: [@https://twitter.com/patrickwardle](https://twitter.com/patrickwardle)

**SpeakerBio:** Tom McGuire

Tom has been working in the security industry since the late 90s. He is the CTO of a cybersecurity firm and an Instructor at Johns Hopkins University where he teaches Reverse Engineering, OS Security, Cryptology and Cyber Risk Management. He loves his family, all things security, biotech and the Red Sox!

### Description:

In an ideal world, members of a community work together towards a common goal or greater good. Unfortunately, we do not (yet) live in such a world.

In this talk, we discuss what appears to be a systemic issue impacting our cyber-security community: the theft and unauthorized use of algorithms by corporate entities. Entities who themselves may be part of the community.

First, we'll present a variety of search techniques that can automatically point to unauthorized code in commercial products. Then we'll show how reverse-engineering and binary comparison techniques can confirm such findings.

Next, we will apply these approaches in a real-world case study. Specifically, we'll focus on a popular tool from a non-profit organization that was reverse-engineered by multiple entities such that its core algorithm could be recovered and used (unauthorized), in multiple commercial products.

The talk will end with actionable takeaways and recommendations, as who knows, this may happen to you too! For one, we'll present strategic approaches (and the challenges) of confronting culpable commercial entities (and their legal teams).

Moreover, we'll provide recommendations for corporations to ensure this doesn't happen in the first place, thus ensuring that our community can remain cohesively focused on its mutual goals.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## SKY - Saturday - 16:00-16:50 PDT

---

**Title:** Dancing Around DRM

**When:** Saturday, Aug 13, 16:00 - 16:50 PDT

**Where:** LINQ - BLOQ

**Speakers:** Game Tech Chris,

**SpeakerBio:** Game Tech Chris

No BIO available

Twitter: [@https://twitter.com/gtc](https://twitter.com/gtc)

**SpeakerBio:**

No BIO available

Twitter: [@https://twitter.com/lobstar85](https://twitter.com/lobstar85)

### **Description:**

After losing hundreds of pounds playing dance dance revolution (seriously, over 300 pounds down!), it was discovered that this game had suicide DRM - when the hard drive dies, it's game over; You could not get it repaired! Two friends set out on a journey to tear the game apart and find a way to keep dancing after the components have sunset. This is the story of how this game (and others that used the same protection scheme) was saved without fully needing to break their entire DRM scheme!

This talk will go over the hardware and software combination approach we used to combat a notorious DRM scheme and preserve a series of arcade games. The protection is employed in commercial and consumer environments and this trick has been used to preserve not only these, but many other digital games from extinction.

---

[Return to Index](#) - Add to



- ics [Calendar](#) file

---

## **MIV - Friday - 11:30-13:30 PDT**

---

**Title:** Dazed and Seriously Confused: Analysis of Data Voids & the Disinformation Landscape of Central Asia

**When:** Friday, Aug 12, 11:30 - 13:30 PDT

**Where:** Caesars Forum - Summit 221->236

**SpeakerBio:** Rhyner Washburn

Rhyner Washburn is a Cyber Intelligence Researcher at the National Consortium for the Study of Terrorism and Responses to Terrorism (START), based at the University of Maryland. His research focuses on cybersecurity, international security, terrorism, and the intersection of those topics. His expertise includes multi-domain influence and critical infrastructure attack operations; and Chinese and North Korean cyber operations.

**Description:** No Description available

---

[Return to Index](#) - Add to



- ics [Calendar](#) file

---

## **SOC - Friday - 16:00-18:59 PDT**

---

**Title:** DC404/DC678/DC770/DC470 (Atlanta Metro) Meetup

**When:** Friday, Aug 12, 16:00 - 18:59 PDT

**Where:** Caesars Forum - Summit 211-213

## 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 (or interested in!) DC404's 20+ year legacy can catch up, share stories, and make new connections. Come prepared to share your interests, hacks, swag, stories, and good times!

---

[Return to Index](#) - Add to



- ics [Calendar](#) file

---

## SOC - Thursday - 18:00-20:59 PDT

---

**Title:** DC702 Pwnagotchi Party

**When:** Thursday, Aug 11, 18:00 - 20:59 PDT

**Where:** Caesars Forum - Summit 211-213

## Description:

Join DC702 for a Pwnagotchi party. The DC702 team will be auctioning off kits and donating the proceeds to the EFF, as well as providing instructions and guidance for assembly. Everyone is welcome to come by, and if you have your own assembled or unassembled kit, feel free to bring it!

---

[Return to Index](#) - Add to



- ics [Calendar](#) file

---

## ASV - Friday - 11:30-11:55 PDT

---

**Title:** DDS Space Signal Lab

**When:** Friday, Aug 12, 11:30 - 11:55 PDT

**Where:** Caesars Forum - Forum 112-117

**SpeakerBio:** James Pavur , Digital Service Expert, Defense Digital Service

Dr. James Pavur is a Digital Service Expert at the DoD Directorate of Digital Services where he advises and assists the US Department of Defense in implementing modern digital solutions to urgent and novel challenges. Prior to joining DDS, James received his PhD. from Oxford University's Department of Computer Science as a Rhodes Scholar. His thesis "Securing New Space: On Satellite Cybersecurity" focused on the security of modern space platforms - with a particular interest in vulnerability identification and remediation. His previous research on satellite security has been published at top academic venues, such as IEEE S&P and NDSS, presented at major cybersecurity conferences, including Black Hat USA and DEFCON, and covered in the popular press. Outside of tech, James enjoys flying kites and collecting rare and interesting teas.

Twitter: [@https://twitter.com/jamespavur](https://twitter.com/jamespavur)

## Description:

The goal of this demo lab is to teach participants that radio signals can often be received and interpreted by people who aren't their intended recipients. A secondary objective is to explore the consequences of that in the context of other critical infrastructure and convey why privacy in SATCOMs matters.

---

[Return to Index](#) - Add to



- ics [Calendar](#) file

---

## DDV - Friday - 10:00-16:59 PDT

---

**Title:** DDV open and accepting drives for duplication

**When:** Friday, Aug 12, 10:00 - 16:59 PDT

**Where:** Flamingo - Exec Conf Ctr - Lake Meade and Valley of Fire

### Description:

We reopen and accept 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. 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 Calendar](#) - ics [Calendar](#) file

---

## DDV - Saturday - 10:00-16:59 PDT

---

**Title:** DDV open and accepting drives for duplication

**When:** Saturday, Aug 13, 10:00 - 16:59 PDT

**Where:** Flamingo - Exec Conf Ctr - Lake Meade and Valley of Fire

### Description:

We reopen and accept 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. 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 Calendar](#) - ics [Calendar](#) file

---

## DDV - Thursday - 16:00-18:59 PDT

---

**Title:** DDV starts accepting drives for duplication

**When:** Thursday, Aug 11, 16:00 - 18:59 PDT

**Where:** Flamingo - Exec Conf Ctr - Lake Meade and Valley of Fire

### Description:

We start taking drives at 4:00pm local time on Thursday, August 11th. 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. 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 Calendar](#) - ics [Calendar](#) file

---

## SKY - Friday - 17:05-17:55 PDT

---

**Title:** Deadly Russian Malware in Ukraine

**When:** Friday, Aug 12, 17:05 - 17:55 PDT

**Where:** LINQ - BLOQ

**SpeakerBio:**Chris Kubecka

CEO of cyber warfare incident management company in The Netherlands and Distinguished Chair for a Cyber Security program in the US Program. Advises the multiple governments, militaries, television and documentary technical advisor as a subject matter expert on cyber warfare national defense. Author of OSINT books and USAF military combat veteran, former military aircrew, and USAF Space Command. Defends critical infrastructure and handles country level cyber incidents, cyberwarfare, and cyber espionage. Lives and breathes IT/IOT/ICS SCADA control systems security. Hacker since the age of 10 and was in Kiev when the war started.

Twitter: [@https://twitter.com/SecEvangelism](https://twitter.com/SecEvangelism)

**Description:**

Has Russian malware lead to loss of life, yes. The effects of the Ukrainian border patrol and orphan database wiper viruses. Russian malware pinpointing evacuating refugees for murder. Wiping orphan identifications so they can't escape the Mariupol, killing many in the theater they sheltered in. Wiping border control to the point they operated on pen and paper, slowing evacuations leaving some to freeze to death desperate to flee. Luring of humanitarian aid workers through surveillanceware and misinformation leading to kidnapping and ransom payments with cryptocurrency. Targeting refugees in Europe for surveillance, harassment and intimidation. No digital ID, no cash, no credit cards. What happens when cyberwar affects everyday lives.

[Return to Index](#) - Add to



- ics [Calendar](#) file

## DC - Friday - 17:30-17:50 PDT

**Title:** Deanonymization of TOR HTTP hidden services

**When:** Friday, Aug 12, 17:30 - 17:50 PDT

**Where:** Caesars Forum - Alliance 301-309, 321 (Track 4)

**SpeakerBio:**Ionut Cernica , PHD Student Department of Computer Science, Faculty of Automatic Control and Computer Science, University Politehnica of Bucharest

Ionut Cernica started his security career with the bug bounty program from Facebook. His passion for security led him to get involved in dozens of such programs and he found problems in very large companies such as Google, Microsoft, Yahoo, AT&T, eBay, VMware. He has also been testing web application security for 9 years and has had many projects on the penetration testing side.

Another stage of his career was to get involved in security contests and participated in more than 100 such contests. He also reached important finals such as Codegate, Trend Micro and Defcon with the PwnThyBytes team. He also won several individual competitions, including the mini CTF from the first edition of Appsec village - Defcon village.

Now he is doing research in the field of web application security, being also a PhD student at University Polytechnic of Bucharest. Through his research he wants to innovate in the field and to bring a new layer of security to web applications.

Twitter: [@https://twitter.com/Cernicalonut](https://twitter.com/Cernicalonut)

**Description:**

Anonymity networks such as Tor are used to protect the identity of people or services. Several deanonymization techniques have been described over time. Some of them attacked the protocol, others exploited various configuration issues. Through this presentation I will focus on deanonymization techniques of the http services of such networks by exploiting configuration issues.

In the first part of the presentation, I will present deanonymization techniques on TOR which are public, and I will also present the techniques developed by me and the interesting story of how I came to develop them.

In the last part of my presentation, I will do a demo with the exploitation of http hidden services in TOR and I will present each technique separately. I will also present how one of the techniques can be used successfully not only in the TOR network, but also on the internet in order to obtain information about the server that will help you discover other services.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## BICV - Saturday - 12:00-12:30 PDT

---

**Title:** Decolonizing Cybersecurity

**When:** Saturday, Aug 13, 12:00 - 12:30 PDT

**Where:** Virtual - BIC Village

**SpeakerBio:** Birhanu Eshete

No BIO available

**Description:** No Description available

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## CLV - Sunday - 11:50-12:30 PDT

---

**Title:** Deescalate the overly-permissive IAM

**When:** Sunday, Aug 14, 11:50 - 12:30 PDT

**Where:** Flamingo - Scenic Ballroom

**SpeakerBio:** Jay Chen

Jay Chen is a security researcher with Palo Alto Networks. He has extensive research experience in cloud-native, public clouds, and edge computing. His current research focuses on investigating the vulnerabilities, design flaws, and adversary tactics in cloud-native technologies. In the past, he also researched Blockchain and mobile cloud security. Jay has authored 20+ academic and industrial papers.

**Description:**

The principle of least privilege states that a subject should be given only those privileges needed for it to complete its task. The concept is not new, but our recent research on 18,000 production cloud accounts across AWS and Azure showed that 99% of the cloud identities were overly-permissive. The majority of the identities only used less than 10% of their granted permissions. While I investigated the issue further, one interesting pattern quickly surfaced, many overly-permissive permissions were granted by CSP-managed permission policies. CSP-managed policies were granted 2.5 times more permissions than customer-managed policies. These excessive permissions unnecessarily increased the attack surface and risks of the cloud workloads. In particular, many identities could abuse the granted permissions to obtain admin privilege.

These findings raised a few questions. Are we all doing something terribly wrong? Is the principle of least privilege a realistic and necessary goal in modern cloud environments? What can be done to mitigate the problem? Knowing the problem and the risks, I will then introduce an open-source tool IAM-Deescalate to shine a light on the problem.

IAM-Deescale can help identify and mitigate the privilege escalation risks in AWS. It models the relationship between every user and role in an AWS account as a graph using PMapper. It then identifies the possible privilege escalation paths that allow non-admin principals to reach admin principals. For each path, IAM-Deescale revokes a minimal set of permissions to break the path to remediate the risks. At the time of writing, IAM-Deescale can remediate 24 out of the 31 publicly known privilege escalation techniques. On average, it remediates 75% of the privilege escalation vulnerabilities that existing open-source tools can detect.

The audience will gain a new perspective on IAM security and pick up a new tool for their security toolbox.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## SOC - Friday - 06:00-05:59 PDT

---

**Title:** DEF CON Bike Ride "CycleOverride"

**When:** Friday, Aug 12, 06:00 - 05:59 PDT

**Where:** Other/See Description

### Description:

At 6am on Friday, the cycle\_override crew will be hosting the 10th Defcon Bikeride. We miscounted last year which was really the 9th. 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 at 6am Friday! jp\_bourget gdead heidishmoo. Go to cycleoverride.org for more info. In the event that there is no on site Defcon, we will do a virtual ride during Defcon.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## DC - Sunday - 15:30-17:30 PDT

---

**Title:** DEF CON Closing Ceremonies & Awards

**When:** Sunday, Aug 14, 15:30 - 17:30 PDT

**Where:** Caesars Forum - Forum 104-110, 135-136, 138-139 (Tracks 1+2)

**SpeakerBio:** The Dark Tangent , DEF CON

No BIO available

### Description:

DEF CON Closing Ceremonies & Awards, the Uber Black badges are awarded to the winners of CTF and several other contests that earned a Black badge for DEF CON 30! We will wrap up the con, say thanks where it's due, and acknowledge special moments.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## SOC - Friday - 16:00-18:59 PDT

---

**Title:** DEF CON Holland DC3115 & DC3120 Group Meetup

**When:** Friday, Aug 12, 16:00 - 18:59 PDT

**Where:** Flamingo - Bird Bar

### Description:

In The Netherlands it's a tradition to catch up with your colleagues just before the end of the workday on Friday when the weekend starts to kick in. In The Netherlands this is called the "VrijMiBo" (Vrijdag/Friday - Middag/Afternoon Borrel/Drink)

"VrijMiBo/Friday afternoon Drink" at DefCon is a perfect moment to talk about what your favorite thing is at DefCon, show your cool handmade badges, impress other hackers about your latest hacks, make new friends, gossip about your boss and show your cat or dog pictures.

Vrijdag Middag Borrel, Freitag Mittags Getränk, Apéritif du vendredi après-midi, trago de viernes por la tarde.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## DC - Friday - 16:30-17:15 PDT

---

**Title:** DEF CON Policy Dept - Special Edition Policy Talk

**When:** Friday, Aug 12, 16:30 - 17:15 PDT

**Where:** Caesars Forum - Forum 106-110, 138-139 (Track 2)

**SpeakerBio:**DEF CON Policy Dept

No BIO available

**Description:**No Description available

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## DC - Friday - 17:30-18:15 PDT

---

**Title:** DEF CON Policy Dept - Special Edition Policy Talk

**When:** Friday, Aug 12, 17:30 - 18:15 PDT

**Where:** Caesars Forum - Forum 106-110, 138-139 (Track 2)

**SpeakerBio:**DEF CON Policy Dept

No BIO available

**Description:**No Description available

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## DC - Friday - 12:30-13:15 PDT

---

**Title:** DEF CON Policy Dept - Special Edition Policy Talk

**When:** Friday, Aug 12, 12:30 - 13:15 PDT

**Where:** Caesars Forum - Forum 106-110, 138-139 (Track 2)

**SpeakerBio:**DEF CON Policy Dept

No BIO available

**Description:**No Description available

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## DC - Friday - 11:30-12:15 PDT

---

**Title:** DEF CON Policy Dept - Special Edition Policy Talk

**When:** Friday, Aug 12, 11:30 - 12:15 PDT

**Where:** Caesars Forum - Forum 106-110, 138-139 (Track 2)

**SpeakerBio:**DEF CON Policy Dept

No BIO available

**Description:**No Description available

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## DC - Friday - 13:30-14:15 PDT

---

**Title:** DEF CON Policy Dept - Special Edition Policy Talk

**When:** Friday, Aug 12, 13:30 - 14:15 PDT

**Where:** Caesars Forum - Forum 106-110, 138-139 (Track 2)

**SpeakerBio:**DEF CON Policy Dept

No BIO available

**Description:**No Description available

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## DC - Sunday - 12:00-12:45 PDT

---

**Title:** Defaults - the faults. Bypassing android permissions from all protection levels

**When:** Sunday, Aug 14, 12:00 - 12:45 PDT

**Where:** Caesars Forum - Alliance 301-309, 321 (Track 4)

**SpeakerBio:**Nikita Kurtin , Hacker

By day - senior research developer

By night - street workout athlete

Sometimes vice versa ;-)

Favorite quote: "Between dream and reality, there is only you."

You can see CVE on my name here:

<https://source.android.com/security/overview/acknowledgements>

## Description:

Exploring in depth the android permission mechanism, through different protection levels.

Step by step exploitations techniques that affect more than 98% of all Android devices including the last official release (Android 12).

In this talk I reveal a few different techniques that I uncovered in my research, which can allow hackers to bypass permissions from all protection levels in any Android device, which is more than 3 billion active devices according to the google official stats.

These vulnerabilities enable the hacker to bypass the security measures of android, by abusing default (built in) services and get access to abilities and resources which are protected by permission mechanism.

Some vulnerabilities are partially fixed, others won't be fixed as google considers as intended behavior.

In this talk I'll survey the different vulnerabilities, and deep dive into a few of different exploitations.

Finally, I'll demonstrate how those techniques can be combined together to create real life implications and to use for: Ransomware, Clickjacking, Uninstalling other apps and more, completely undetected by security measures.

---

[Return to Index](#) - Add to



- ics [Calendar](#) file

---

## DC - Saturday - 16:30-17:15 PDT

---

**Title:** Defeating Moving Elements in High Security Keys

**When:** Saturday, Aug 13, 16:30 - 17:15 PDT

**Where:** Caesars Forum - Alliance 301-309, 321 (Track 4)

**SpeakerBio:** Bill Graydon , Principal, Physical Security Analytics, GGR Security

Bill Graydon is a principal researcher at GGR Security, where 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.

Twitter: [@https://twitter.com/access\\_ctrl](https://twitter.com/access_ctrl)

## Description:

A recent trend in high security locks is to add a moving element to the key: this prevents casting, 3D printing and many other forms of unauthorised duplication. Pioneered by the Mul-T-Lock Interactive locks, we see the technique used in recent Mul-T-Lock iterations, the Abloy Protec 2 and most recently, the Medeco M4, which is only rolling out to customers now.

We have identified a major vulnerability in this technology, and have developed a number of techniques to unlock these locks using a key made from a solid piece of material, which defeats all of the benefits of an interactive key. I'll demonstrate how it can be applied to Mul-T-Lock Interactive, Mul-T-Lock MT5+ and the Medeco M4, allowing keys to be duplicated by casting, 3D printing and more. I'll also cover other techniques to defeat moving elements in a key, such as printing a compliant mechanism and printing a captive element directly. With this talk, we're also releasing a web application for anyone to generate 3D printable files based on this exploit. Finally, I'll also discuss the responsible disclosure process, and working with the lock manufacturers to patch the vulnerability and mitigate the risk.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## PT - Monday - 09:00-16:59 PDT

---

**Title:** Defender's Guide to Securing Public Cloud Infrastructures

**When:** Monday, Aug 15, 09:00 - 16:59 PDT

**Where:** Caesars Forum

### **SpeakerBio:** Abhinav Singh

Abhinav Singh is a cybersecurity researcher with close to a decade long experience working for global leaders in security technology, financial institutions and as an independent trainer/consultant. He is the author of Metasploit Penetration Testing Cookbook (first, second & third editions) and Instant Wireshark Starter, by Packt. He is an active contributor to the security community in the form of patents, open-source tools, paper publications, articles, and blogs. His work has been quoted in several security and privacy magazines, and digital portals. He is a frequent speaker at eminent international conferences like Black Hat, RSA & Defcon. His areas of expertise include malware research, reverse engineering, enterprise security, forensics, and cloud security.

### **Description:**

Latest details, requirements, description, cost:

<https://defcontrainings.myshopify.com/products/abhinav-singh-defenders-guide-to-securing-public-cloud-infrastructures>

Training description:

This training focuses on elevating your threat detection, investigations, and response knowledge into the cloud. This hands-on training simulates real-life attack scenarios on cloud infrastructure & applications. It then teaches you to build your own defensive tools against such attacks by using cloud native services on AWS. This makes it an ideal class for red & blue teams.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## PT - Tuesday - 09:00-16:59 PDT

---

**Title:** Defender's Guide to Securing Public Cloud Infrastructures

**When:** Tuesday, Aug 16, 09:00 - 16:59 PDT

**Where:** Caesars Forum

### **SpeakerBio:** Abhinav Singh

Abhinav Singh is a cybersecurity researcher with close to a decade long experience working for global leaders in security technology, financial institutions and as an independent trainer/consultant. He is the author of Metasploit Penetration Testing Cookbook (first, second & third editions) and Instant Wireshark Starter, by Packt. He is an active contributor to the security community in the form of patents, open-source tools, paper publications, articles, and blogs. His work has been quoted in

several security and privacy magazines, and digital portals. He is a frequent speaker at eminent international conferences like Black Hat, RSA & Defcon. His areas of expertise include malware research, reverse engineering, enterprise security, forensics, and cloud security.

## Description:

Latest details, requirements, description, cost:

<https://defcontrainings.myshopify.com/products/abhinav-singh-defenders-guide-to-securing-public-cloud-infrastructures>

Training description:

This training focuses on elevating your threat detection, investigations, and response knowledge into the cloud. This hands-on training simulates real-life attack scenarios on cloud infrastructure & applications. It then teaches you to build your own defensive tools against such attacks by using cloud native services on AWS. This makes it an ideal class for red & blue teams.

---

[Return to Index](#) - Add to



- ics [Calendar file](#)

---

## PLV - Friday - 14:00-15:45 PDT

---

**Title:** Defense Through a TAC (Technical Advisory Committee)

**When:** Friday, Aug 12, 14:00 - 15:45 PDT

**Where:** Caesars Forum - Summit 226-227 - Policy Roundtable

**SpeakerBio:** The Dark Tangent , DEF CON

No BIO available

## Description:

CISA invited hackers to weigh in on difficult challenges across the cybersecurity ecosystem. Learn what they're doing and help shape what could come next. The CISA Cybersecurity Advisory Committee (CSAC) Technical Advisory Committee (TAC) was chartered to bring hackers in to raise and address difficult challenges across the cybersecurity ecosystem.

Attendees will learn what started the TAC, what they're tackling, and what they've produced, and will have the opportunity to engage in substantive conversations on the policy topics they think could be most critical to addressing in future sessions.

---

[Return to Index](#) - Add to



- ics [Calendar file](#)

---

## DL - Saturday - 12:00-13:55 PDT

---

**Title:** Defensive 5G

**When:** Saturday, Aug 13, 12:00 - 13:55 PDT

**Where:** Caesars Forum - Council Boardroom

**Speakers:**Ryan Ashley,Eric Mair

**SpeakerBio:**Ryan Ashley

Ryan Ashley is currently a senior software-engineer at In-Q-Tel Labs. He is responsible for architecture, design, and implementation of open-source tools for analysis and visualization of network activity and other cyber-security use-cases. He is the primary maintainer of the IQT-Labs project NetworkML, and is a contributor to various other open-source projects.

**SpeakerBio:**Eric Mair

Eric Mair has been working in wireless communications for over 20 years and is currently working for In- Q-Tel Labs in Arlington, VA as a senior communications-technologist focusing on 5G, SDR and the application of machine-learning to RF communications. Prior to IQT he was with the US Government for 19 years.

## Description:

In this work we developed a 4.5G/5G network using only commercial off the shelf (COTS) hardware and open-source software to serve as test-infrastructure for studying vulnerabilities in 5G networks. We are using software defined networking (SDN) tools such as Faucet and Dovesnap and software defined radio(SDR) capabilities such as Open5gs and srsRAN along with Docker Containers to facilitate the rapid and reliable setup and configuration of network topologies that can be used to represent the 5G networks that we intend to test. By having a configurable and repeatable mechanism that could be shared among multiple users with differing hardware setups we were able to test 5G network configurations in a variety of ways and have those results validated by other team members.

Audience: Target Audience: Network Defense and Attack, 5G, Software Defined Radio and Infrastructure-as-Code.

---

[Return to Index](#) - Add to [!\[\]\(8a7d1420c8b61860c664aba460a75ead\_img.jpg\) Google Calendar](#) - ics [Calendar](#) file

---

## BICV - Friday - 14:00-14:30 PDT

---

**Title:** DEI in Cybersecurity (Breaking through the barrier, behind the barrier... behind the barrier)

**When:** Friday, Aug 12, 14:00 - 14:30 PDT

**Where:** Virtual - BIC Village

**SpeakerBio:** Damian Grant

No BIO available

**Description:** No Description available

---

[Return to Index](#) - Add to [!\[\]\(f86a80153bf8bed9942beb868990bfab\_img.jpg\) Google Calendar](#) - ics [Calendar](#) file

---

## SOC - Saturday - 17:00-18:59 PDT

---

**Title:** Denial, Deception, and Drinks with Mitre Engage

**When:** Saturday, Aug 13, 17:00 - 18:59 PDT

**Where:** Caesars Forum - Society Boardroom

## Description:

Interested in cyber denial, deception, and adversary engagement? Come join the MITRE Engage team for conversations, war stories, and cyber shenanigans.

---

[Return to Index](#) - Add to [!\[\]\(b39c9d61b1c9ee35179257beaf4e11c9\_img.jpg\) Google Calendar](#) - ics [Calendar](#) file

---

## BHV - Friday - 11:30-11:59 PDT

---

**Title:** Department of Defense 5G Telemedicine and Medical Training: The Future of Healthcare the Remote Warrior

**When:** Friday, Aug 12, 11:30 - 11:59 PDT

**Where:** Flamingo - Laughlin I,II,III

**SpeakerBio:** Paul Young , MD

No BIO available

**Description:** No Description available

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## MIV - Friday - 11:30-13:30 PDT

---

**Title:** Detecting the "Fake News" Before It Was Even Written, Media Literacy, and Flattening the Curve of the COVID-19 Infodemic

**When:** Friday, Aug 12, 11:30 - 13:30 PDT

**Where:** Caesars Forum - Summit 221->236

**SpeakerBio:** Preslav Nakov

Dr. Preslav Nakov leads the Tanbih mega-project (<http://tanbih.qcri.org/>), developed in collaboration with MIT. The project's aim is to build a news aggregator that limits the effect of fake news, propaganda and media bias by helping users step out of their bubble and achieve a healthy news diet. He is also the lead-PI of a QCRI-MIT collaboration project on Arabic Speech and Language Processing for Cross-Language Information Search and Fact Verification, and he was a co-PI of another QCRI-MIT collaboration project on Speech and Language Processing for Arabic (2013-2016). Dr. Nakov is Secretary of ACL SIGLEX and also a Secretary of ACL SIGSLAV.

**Description:** No Description available

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## WS - Friday - 10:00-13:59 PDT

---

**Title:** DFIR Against the Digital Darkness: An Intro to Forensicking Evil

**When:** Friday, Aug 12, 10:00 - 13:59 PDT

**Where:** Harrah's - Reno

**Speakers:** Michael Register, Michael Solomon

**SpeakerBio:** Michael Register , Threat Hunter

Michael Register (S3curityNerd) has 6 years of combined experience across IT, Networking, and Cybersecurity.

S3curityNerd joined the cybersecurity space in 2017 and has worked in multiple roles, including his current one as a Threat Hunter. He enjoys both learning new things and sharing new things with others.

**SpeakerBio:** Michael Solomon , Threat Hunter

Michael Solomon (mR\_F0r3n51c5) is a Threat Hunter for a large managed security service provider. He has 12 years of experience conducting Cyber Operations, Digital Forensics & Incident Response (DFIR), and Threat Hunting. He is very passionate about helping grow and inspire cybersecurity analysts for a better tomorrow.

## Description:

Ever wondered what it is like being a cybersecurity or incident response analyst? Are you new to investigation or want to take your analysis to the next level? If you answered yes, here is your chance to experience an exciting 4-hour class taught by mR\_F0r3n51c5 and S3curityNerd. In today's threat landscape, malware continues to be used by all various types of threat actors. This class teaches students how to investigate a compromised Windows system using forensic and malware analysis fundamentals.

Upon successful class completion, students will be able to: - Build analysis skills that leverage complex scenarios and improve comprehension. - Practically acquire data in a forensically sound manner. - Identify common areas of malware persistence. - Gather evidence and create a timeline to characterize how the system was compromised. - Participate in a hand to keyboard combat capstone. Students are given an image of a compromised Windows system and demonstrate how to analyze it.

## Materials

Students will be required to download a virtual machine (OVA file). Students will be given a URL for download access. Regarding the downloaded virtual machine, this will be imported into your virtual machine software and ready before the start of class. If any additional technical support is needed, the instructors will make themselves available online. Students must have a laptop that meets the following requirements: A 64 bit CPU running at 2GHz or more. The students will be running a virtual machine on their host laptop. Have the ability to update BIOS settings. Specifically, enable virtualization technology such as "Intel-VT." The student must be able to access their system's BIOS if it is password protected. This is in case of changes being necessary. 8 GB (Gigabytes) of RAM or higher At least one open and working USB Type-A port 50 Gigabytes of free hard drive space, allowing you the ability to host the VMs we distribute Students must have Local Administrator Access on their system. Wireless 802.11 Capability A host operating system that is running Windows 10+, Linux, or macOS 10.4 or later. Virtualization software is required. The supplied VM has been built for out-of-the-box comparability with VMWare Workstation or Player. Students may use other software if they choose, but they may have to troubleshoot unpredictable issues. At a minimum, the following VM features will be needed: NATted networking from VM to Internet Copy Paste of text and files between the Host machine and VM

## Prereq

Although no prerequisites are required, experience with using virtual machines will be helpful.

---

[Return to Index](#) - Add to



- ics [Calendar](#) file

---

## WS - Saturday - 10:00-13:59 PDT

---

**Title:** Dig Dug: The Lost Art of Network Tunneling

**When:** Saturday, Aug 13, 10:00 - 13:59 PDT

**Where:** Harrah's - Lake Tahoe

**Speakers:**Elijah,Cam

**SpeakerBio:**Elijah , Founder

Elijah is the founder of Code Siren, LLC and has 20+ years of software development and security experience. He is also the creator of Demonsaw, an encrypted communications platform that allows you to chat, message, and transfer files without fear of data collection or surveillance. Before that Elijah was a Lead Programmer at Rockstar Games where he created games like Grand Theft Auto V and Red Dead Redemption 2. In 2007, Elijah 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. Elijah is an active member of the hacking community and is an avid proponent of Internet freedom.

**SpeakerBio:**Cam , Developer, Hacker

Cam is a developer and hacker with experience in C++, Java, and Android. He has spent the past 5 years writing software for secure communication platforms including VOIP and messaging services. In his free time, he enjoys Android reverse engineering, studying Mandarin, and writing software for human rights projects.

## Description:

In a world of decreasing privacy, it's important that users can communicate P2P without any reliance on centralized solutions. But how do computers connect directly to each other without having external IP addresses, using an insecure protocol like UPnP, manually port forwarding, or routing through intermediary services like Signal, Skype, or Telegram? The traditional solution to this problem has been to trust companies and just route our data through their servers. We can totally trust them, right? If the future of secure communication depends on companies to route our traffic, then I would argue that the future of communications is insecure. There must be a better solution more in line with privacy fundamentals.

Reverse Network Tunneling, i.e. UDP Hole Punching, is a powerful technique that makes it possible for computers with internal IP addresses that are inaccessible on the Internet to be able to connect to each other directly, and therefore become accessible. As crazy as this sounds, it's real and works. This has multiple applications in the real world, such as allowing a pentester to directly connect to a victim that is hidden behind a router. Network tunneling also invalidates the need of centralized services provided by companies that log, surveil and profit from our traffic. Imagine how the future of secure communications would change if all of our online interactions were off-the-grid?

This workshop shows you how to punch holes through external routers to allow computers that were once hidden from the Internet to connect to each other P2P. If you've ever wanted to tunnel into private networks and access internal computers, then this workshop is for you. Create a botnet, backdoor, or even the next great privacy app - the sky's the limit! This is a beginner-level, technical workshop and requires that attendees have some prior experience in at least one programming language, such as Python, JavaScript or C++. Bring your laptop and a strong appetite for pwning network devices.

### Materials

Laptop with Windows, Linux, or OSX. USB flash drive for copying program materials (optional).

### Prereq

Previous experience in at least one programming language is required. Previous experience with Python or C/C++ is recommended, but not required.

---

[Return to Index](#) - Add to



- ics [Calendar](#) file

---

## DC - Saturday - 14:30-14:50 PDT

---

**Title:** Digging into Xiaomi's TEE to get to Chinese money

**When:** Saturday, Aug 13, 14:30 - 14:50 PDT

**Where:** Caesars Forum - Forum 106-110, 138-139 (Track 2)

**SpeakerBio:** Slava Makkaveev , Security Researcher, Check Point

Slava Makkaveev is a Security Researcher at Check Point Research. Holds a PhD in Computer Science. Slava has found himself in the security field more than ten years ago and since that gained vast experience in reverse engineering and vulnerability research. Recently Slava has taken a particularly strong interest in mobile platforms and firmware security. Slava was a speaker at DEF CON, CanSecWest, RECon, HITB and others.

## Description:

The Far East and China account for two-thirds of global mobile payments in 2021. That is about \$4 billion in mobile wallet transactions. Such a huge amount of money is sure to attract the attention of hackers. Have you ever wondered how safe it is to pay from a mobile device? Can a malicious app steal money from your digital wallet? To answer these questions, we researched the payment system built into Xiaomi smartphones based on MediaTek chips, which are very popular in China. As a result, we discovered vulnerabilities that allow forging payment packages or disabling the payment system directly from an

unprivileged Android application.

Mobile payment signatures are carried out in the Trusted Execution Environment (TEE) that remains secure on compromised devices. The attacker needs to hack the TEE in order to hack the payment. There is a lot of good research about mobile TEEs in the public domain, but no one pays attention to trusted apps written by device vendors like Xiaomi and not by chip makers, while the core of mobile payments is implemented there. In our research, we reviewed Xiaomi's TEE for security issues in order to find a way to scam WeChat Pay.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## DC - Saturday - 18:30-18:50 PDT

---

**Title:** Digital Skeleton Keys - We've got a bone to pick with offline Access Control Systems

**When:** Saturday, Aug 13, 18:30 - 18:50 PDT

**Where:** Caesars Forum - Alliance 301-309, 321 (Track 4)

**Speakers:**Miana E Windall,Micsen

**SpeakerBio:**Miana E Windall , Software Development Engineer

Miana is a lifelong tinkerer who likes breaking things almost as much as she likes building them.

Twitter: [@https://twitter.com/NiamhAstra](https://twitter.com/NiamhAstra)

**SpeakerBio:**Micsen , Software developer, Installer, And much more!

Micsen: At 5 years old Micsen began his career of dismantling things. He had just gotten his first RC car and wanted to fix it since it didn't drive straight. Luckily the skills have evolved significantly from that time as the car never drove again! When a company is affected by ransomware he will happily use his hacking skills to trade for booze.

Twitter: [@https://twitter.com/micsen97](https://twitter.com/micsen97)

### Description:

Offline RFID systems rely on data stored within the key to control access and configuration. But what if a key lies? What if we can make the system trust those lies? Well then we can do some real spooky things... This is the story of how a strange repeating data pattern turned into a skeleton key that can open an entire range of RFID access control products in seconds.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## BHV - Friday - 13:30-13:59 PDT

---

**Title:** DIY Medicine With Unusual Uses for Existing FDA-Approved Drugs

**When:** Friday, Aug 12, 13:30 - 13:59 PDT

**Where:** Flamingo - Laughlin I,II,III

**SpeakerBio:**Mixael S. Laufer

Mixael Swan Laufer worked in mathematics and high energy physics until he decided to use his background in science to tackle problems of global health and human rights. He continues to work to make it possible for people to manufacture their own medications and medical devices at home by creating public access to tools, ideas, and information.

Twitter: [@https://twitter.com/MichaelSLaufer](https://twitter.com/MichaelSLaufer)

### Description:

Not only are there plenty of cures and treatments which stay on the shelf, inaccessible because they were never approved by the FDA, but there are also drugs which have already been approved, but are not generally prescribed for their best uses. Viagra cures menstrual cramps better than it treats ED, but doctors will not prescribe it for that. There is a decades-old substance which arrests and fixes tooth decay without drilling, approved by the ADA, but no dentist will ever tell you about it. You can easily give yourself an abortion with existing ulcer drugs, but they require a trick to acquire. Anxiety, depression, poor sleep, and bad digestion are all linked to GABA deficiency, which often has its roots in the deficiency of a precursor which only comes from gut bacteria. You can repopulate your gut with those bacteria with supplements which are GRAS [FDA designation: generally recognized as safe], cheap and not patented; but for this exact reason, you're much more likely to instead be prescribed zoloft, valium, protonix, and ambien. The medical industry seems be ignoring long covid while there is a decades-old drug for a rare disease which can cure most autoimmune-presenting instances of long covid. Come see all this and more, as we show you how to hack medicines which are already on the shelf.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## BHV - Friday - 14:30-15:59 PDT

---

**Title:** DIY MQTT IoT (or how you can turn your home into an interconnected palace of human-centric data)

**When:** Friday, Aug 12, 14:30 - 15:59 PDT

**Where:** Flamingo - Laughlin I,II,III

**SpeakerBio:**Cody Wayne Burkhart

No BIO available

**Description:**No Description available

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## PLV - Saturday - 19:00-21:59 PDT

---

**Title:** Do No Harm (Lounge)

**When:** Saturday, Aug 13, 19:00 - 21:59 PDT

**Where:** Caesars Forum - Summit 226-227 - Policy Roundtable

**Speakers:**Seeyew Mo,Jessica Wilkerson,Jeff "r3plicant" Tully MD,Christian "quaddi" Dameff MD,Alissa Knight

**SpeakerBio:**Seeyew Mo , Senior Cybersecurity, Tech, National Security Fellow

No BIO available

**SpeakerBio:**Jessica Wilkerson , Cyber Policy Advisor at the US Food and Drug Administration FDA

No BIO available

**SpeakerBio:**Jeff "r3plicant" Tully MD , Anesthesiologist at The University of California San Diego

Jeff (r3plicant) Tully is a security researcher with an interest in understanding the ever-growing intersections between healthcare and technology. His day job focuses primarily on the delivery of oxygen to tissues.

Twitter: [@https://twitter.com/JeffTullyMD](https://twitter.com/JeffTullyMD)

**SpeakerBio:**Christian "quaddi" Dameff MD , Emergency Medicine Physician & Hacker at The University of California San Diego

Christian (quaddi) Dameff MD is an Assistant Professor of Emergency Medicine, Biomedical Informatics, and Computer Science (Affiliate) at the University of California San Diego. He is also a hacker, former open capture the flag champion, and prior DEF CON/RSA/Blackhat/HIMSS speaker. Published works include topics such as therapeutic hypothermia after cardiac arrest, novel drug targets for myocardial infarction patients, and other Emergency Medicine related works. Published security research topics including hacking critical healthcare infrastructure, medical devices and the effects of malware on patient care. This is his eighteenth DEF CON.

Twitter: <https://twitter.com/CDameffMD>

**SpeakerBio:** Alissa Knight , Hacker & principal analyst at Alissa Knight & Associates

No BIO available

## Description:

Hackers in healthcare have come a long way from the days of the Manifesto. There is no longer apathy amongst the powerful - baby food has been replaced with steak. Hackers are making medical devices safer for patients. Hackers are protecting hospitals from ransomware. Hackers are writing policy and guiding regulation. This is cause for celebration- and where better to throw down than DEF CON 30?

Let's face it- the last couple of years have been doom and gloom, and while attacks on hospitals continue to increase at record pace, and the promise of new medical technologies is equally matched with some terrifying security implications (Neuralink, call us), we really do need to stand back and appreciate where we've come from, because only then can we put into perspective what we still need to do.

D0 No H4rm returns to DEF CON to once again give you the chance to interface directly with some of the biggest names in a domain that just keeps growing in importance. Moderated by physician hackers quaddi and r3plicant, this perennially packed event - with a heavily curated panel of policy badasses, elite hackers, and seasoned clinicians - always fills up fast. So if you want to protect patients, build a safer and more resilient healthcare system, and meet some incredible new friends, then join us. And welcome home.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## DC - Saturday - 13:30-14:15 PDT

---

**Title:** Do Not Trust the ASA, Trojans!

**When:** Saturday, Aug 13, 13:30 - 14:15 PDT

**Where:** Caesars Forum - Alliance 301-309, 321 (Track 4)

**SpeakerBio:** Jacob Baines , Lead Security Researcher, Rapid7

Jacob Baines is a Lead Security Researcher at Rapid7 and a member of the Emergent Threat Response team. As part of his daily duties, Jacob conducts n-day and zero-day vulnerability research on important or impactful systems. He particularly enjoys sharing findings with the security community and developing Metasploit exploits.

Jacob has been active in the Security field for well over a decade. He's held positions as a developer, reverse engineer, and vulnerability researcher. As a vulnerability researcher, Jacob has had the good fortune to publish and present his research which varies from embedded system exploitation, web application attacks, and Windows vulnerabilities.

Twitter: [http://twitter.com/Junior\\_Baines](http://twitter.com/Junior_Baines)

## Description:

Cisco ASA and ASA-X are widely deployed firewalls that are relied upon to protect internal networks from the dangers of the outside world. This key piece of network infrastructure is an obvious point of attack, and a known target for exploitation and implantation by APT such as the Equation Group. Yet it's been a number of years since a new vulnerability has been

published that can provide privileged access to the ASA or the protected internal network. But all good things must come to an end.

In this talk, new vulnerabilities affecting the Cisco ASA will be presented. We'll exploit the firewall, the system's administrators, and the ASA-X FirePOWER module. The result of which should call into question the firewall's trustworthiness.

The talk will focus on the practical exploitation of the ASA using these new vulnerabilities. To that end, new tooling and Metasploit modules will be presented. For IT protectors, mitigation and potential indicators of compromise will also be explored.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## DC - Saturday - 14:30-15:15 PDT

---

**Title:** Doing the Impossible: How I Found Mainframe Buffer Overflows

**When:** Saturday, Aug 13, 14:30 - 15:15 PDT

**Where:** Caesars Forum - Alliance 301-309, 321 (Track 4)

**SpeakerBio:** Jake Labelle , Security Consultant

Jake, a security consultant from Basingstoke, UK, got his hands on a licensed emulator for z/OS over the pandemic , and considering that we have been in and out of lockdown for the past two years, started playing around with it for a fairly good portion of time. As someone who adores the 80s cyber aesthetic, he loves mucking around with it, but also there is nothing legacy about mainframes, docker, node js, python all your modern applications/programs are on there. Over the past year, he has found and reported a number of z/OS LPEs and RCEs vulns to IBM.

Twitter: [@https://twitter.com/Jabellz2](https://twitter.com/Jabellz2)

### Description:

Mainframes run the world, literally. Have you ever paid for something, a mainframe was involved, flown? Used a bank? Gone to college? A mainframe was involved. Do you live in a country with a government? Mainframes! The current (and really only) mainframe OS is z/OS from IBM. If you've ever talked to a mainframer you'll get told how they're more secure because buffer overflows are (were) impossible. This talk will prove them all wrong!

Finding exploits on z/OS is no different than any other platform. This talk will walk through how you too can become a mainframe exploit researcher!

Remote code execution is extra tricky on a mainframe as almost all sockets read data with the ASCII character set and convert that to EBCDIC for the application. With this talk you will find out how to find and then remotely overflow a vulnerable mainframe C program and create a ASCII -> EBCDIC shellcode to escalate your privileges remotely, without auth. Previous mainframe talks focused on infrastructure based attacks. This talk builds on those but adds a class of vulnerabilities, opening up the mainframe hacking community.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## SKY - Friday - 13:50-14:40 PDT

---

**Title:** Don't Blow A Fuse: Some Truths about Fusion Centres

**When:** Friday, Aug 12, 13:50 - 14:40 PDT

**Where:** LINQ - BLOQ

**SpeakerBio:**3ncr1pt3d

I am a cyber threat intel analyst who likes to question things, with my work leading to presentations, articles and podcasts. My work history includes KPMG, one of the "Big 4", a major bank, CP Rail, a major railroad, with experience in security audits and assessments, privacy, DRP, project management, vendor management and change management. I am an experienced speaker, and have spoken previously at Skytalks.

**Description:**

How do you harness the power of collaboration when you need it most to protect and defend against threats? You build a fusion center. The concept evolved some 20 years ago in response to countering terrorism post 9/11, and a number of centres were built per the DOJ and DHS. But a few years ago, the concept became the new shiny for banks, a way to keep up with evolving threats and cybercrime. Alas, all that glitters is not gold. Effective fusion centres are powered by trust-enabled collaboration between people. At the end of the day, however, all those flashy lights, big monitors and dazzling graphs don't mean anything without the skilled people who know how to analyze and act on the real information. This talk is a cautionary tale of what's good and bad about fusion centres, with comparisons drawn from my experiences of working in one that really wasn't working well and why we must value our people over our technology.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

**LPV - Sunday - 12:00-12:25 PDT**

---

**Title:** Doors, Cameras, and Mantraps. Oh, my!

**When:** Sunday, Aug 14, 12:00 - 12:25 PDT

**Where:** Caesars Forum - Summit 203-204, 235

**SpeakerBio:**Dylan Baklor

No BIO available

**Description:**

A general, high level talk, about practical physical security assessment.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

**DC - Friday - 18:30-18:50 PDT**

---

**Title:** Dragon Tails: Supply-side Security and International Vulnerability Disclosure Law

**When:** Friday, Aug 12, 18:30 - 18:50 PDT

**Where:** Caesars Forum - Forum 106-110, 138-139 (Track 2)

**Speakers:**Stewart Scott,Trey Herr

**SpeakerBio:**Stewart Scott , Assistant Director

Stewart Scott is an assistant director with the Cyber Statecraft Initiative under the Scowcroft Center for Strategy and Security at the Atlantic Council. His work there focuses on systems security policy, including software supply chain risk management, federal acquisitions processes, and open source software security. He holds a BA in Public Policy and a minor in Applications of Computing from Princeton University.

## **SpeakerBio:**Trey Herr , Director

Trey Herr is the director of the Cyber Statecraft Initiative under the Scowcroft Center for Strategy and Security at the Atlantic Council. His team works on cybersecurity and geopolitics including cloud computing, the security of the internet, supply chain policy, cyber effects on the battlefield, and growing a more capable cybersecurity policy workforce. Previously, he was a senior security strategist with Microsoft handling cloud computing and supply chain security policy as well as a fellow with the Belfer Cybersecurity Project at Harvard Kennedy School and a non-resident fellow with the Hoover Institution at Stanford University. He holds a PhD in Political Science and BS in Musical Theatre and Political Science.

## **Description:**

This talk will present a study of the reliance of proprietary and open source software on Chinese vulnerability research. A difficult political environment for Chinese security researchers became acute when a law requiring vulnerability disclosure to government and banning it to all others but the affected vendor took effect in Sept. 2021. No public evaluation of this law's impact has yet been made. This talk will present results of a quantitative analysis on the changing proportion of Chinese-based disclosures to major software products from Google, Microsoft, Apple, and VMWare alongside several major open source packages. The analysis will measure change over time in response to evolving Chinese legislation, significant divergence from data on the allocation of bug bounty rewards, and notable trends in the kinds of disclosed vulnerabilities. The Chinese research community's prowess is well known, from exploits at the Tianfu Cup to preeminent enterprise labs like Qihoo 360. However, the recent law aiming to give the Chinese government early access to the community's discoveries—and the government's apparent willingness to enforce it even on high-profile corporations as seen in its punishment of Alibaba—demand more thorough scrutiny. This talk will address implications for policy and the wider hacker community.

---

[Return to Index](#) - Add to



- ics [Calendar](#) file

---

## **IOTV - Friday - 10:00-17:59 PDT**

---

**Title:** Drone Hack

**When:** Friday, Aug 12, 10:00 - 17:59 PDT

**Where:** Caesars Forum - Alliance 311, 320

## **Description:**

A handcrafted IoT challenge that will put your skills to the test. Be prepared to hack devices over bluetooth low energy, break into Wi-Fi networks, and exploit binaries. If you avoid the deadly sharks and laser beams you may be able to access smart locks, conduct electronic warfare, and fly drones.

---

[Return to Index](#) - Add to



- ics [Calendar](#) file

---

## **IOTV - Saturday - 10:00-17:59 PDT**

---

**Title:** Drone Hack

**When:** Saturday, Aug 13, 10:00 - 17:59 PDT

**Where:** Caesars Forum - Alliance 311, 320

## **Description:**

A handcrafted IoT challenge that will put your skills to the test. Be prepared to hack devices over bluetooth low energy, break into Wi-Fi networks, and exploit binaries. If you avoid the deadly sharks and laser beams you may be able to access smart locks, conduct electronic warfare, and fly drones.

## IOTV - Sunday - 10:00-12:59 PDT

---

**Title:** Drone Hack

**When:** Sunday, Aug 14, 10:00 - 12:59 PDT

**Where:** Caesars Forum - Alliance 311, 320

### Description:

A handcrafted IoT challenge that will put your skills to the test. Be prepared to hack devices over bluetooth low energy, break into Wi-Fi networks, and exploit binaries. If you avoid the deadly sharks and laser beams you may be able to access smart locks, conduct electronic warfare, and fly drones.

---

## ASV - Sunday - 12:00-12:50 PDT

---

**Title:** Drones and Civil Liberties

**When:** Sunday, Aug 14, 12:00 - 12:50 PDT

**Where:** Caesars Forum - Forum 112-117

### SpeakerBio:

Andrés Arrieta

As Director of Consumer Privacy Engineering, Andrés oversees projects and issues on privacy, competition, and cybersecurity. He has taken a particular interest in the benefits and risks that drones bring.

### Description:

Drones are capable of bringing many benefits to society but they also pose several risks to our civil liberties. With the FAA moving to create rules for BVLOS (mostly commercial operations) there are important privacy issues raised by a future with many commercial drones flying over our heads. Likewise government agencies want to be able to mitigate risks from operator error to use for nefarious purposes. But the powers they ask are broad, cut into civil liberties, and carry no protections

---

## DL - Saturday - 10:00-11:55 PDT

---

**Title:** EDR detection mechanisms and bypass techniques with EDRSandBlast

**When:** Saturday, Aug 13, 10:00 - 11:55 PDT

**Where:** Caesars Forum - Society Boardroom

**Speakers:**Maxime Meignan,Thomas Diot

### SpeakerBio:

Maxime Meignan

Maxime Meignan (@th3m4ks) is a security consultant at Wavestone, based in Paris, since the middle of the last decade. Loving to reverse engineer binaries in both professional and CTF contexts, Maxime has an IDA sticker on the back of his smartphone. And writes this uninteresting fact in his bio. He is currently interested in various fields of security, related to EDR software, Windows internals and Virtualisation Based Security.

## **SpeakerBio:** Thomas Diot

Thomas Diot (Qazeer) is a security consultant at Wavestone, an independent French consulting firm. His work involves a mix of penetration testing, Red / Purple Teams engagements, and Incident Responses with Wavestone CERT-W. Thomas enjoys practicing and improving his skills by playing in CTFs, developing tools, and working on various security projects.

## **Description:**

EDRSandBlast is a tool written in C that implements and industrializes known as well as original bypass techniques to make EDR evasion easier during adversary simulations. Both user-land and kernel-land EDR detection capabilities can be bypassed, using multiple unhooking techniques and a vulnerable signed driver to unregister kernel callbacks and disable the ETW Threat Intelligence provider. Since the initial release, multiple improvements have been implemented in EDRSandBlast: it is now possible to use this toolbox as a library from another attacking tool, new bypasses have been implemented, the embedded vulnerable driver is now interchangeable to increase stealthiness and the use of a pre-built offsets database is no more required! Come discover our tool and its new features, learn (or teach us!) something about EDRs and discuss about the potential improvements to this project.

Audience: Offense, Defense, Windows, EDR

---

[Return to Index](#) - Add to



- ics [Calendar file](#)

---

## **SOC - Friday - 17:00-19:59 PDT**

---

**Title:** EFF Tech Trivia

**When:** Friday, Aug 12, 17:00 - 19:59 PDT

**Where:** Caesars Forum - Summit 206-208, 238, 237, 234

## **Description:**

EFF's team of technology experts have crafted challenging trivia about the fascinating, obscure, and trivial aspects of digital security, online rights, and Internet culture. Competing teams will plumb the unfathomable depths of their knowledge, but only the champion hive mind will claim the First Place Tech Trivia Plaque and EFF swag pack. The second and third place teams will also win great EFF gear.

---

[Return to Index](#) - Add to



- ics [Calendar file](#)

---

## **SOC - Friday - 15:30-16:30 PDT**

---

**Title:** EFF: Reproductive Justice in the Age of Surveillance

**When:** Friday, Aug 12, 15:30 - 16:30 PDT

**Where:** Caesars Forum - Forum 133

## **Description:**

The U.S. Supreme Court sent shockwaves with its decision to overturn protections for reproductive rights (<https://www.eff.org/issues/reproductive-justice>) under Roe v. Wade. In addition to depriving millions of people of a fundamental right, the decision also means that those who seek (<https://www.eff.org/deeplinks/2022/06/security-and-privacy-tips-people-seeking-abortion>), offer (<https://www.eff.org/deeplinks/2022/05/digital-security-and-privacy-tips-those-involved-abortion-access>), or facilitate abortion healthcare must now consider whether law enforcement could access and use previously benign digital data as evidence of a crime. That's an alarming prospect for an increasingly online world without strong privacy protections.

This panel will explore the future of access to healthcare resources, how technologists are working to help people secure their data now, how policymakers in both the private and public sectors can ensure safety and privacy for millions of people—and what you can do to protect yourself and your communities.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## PLV - Friday - 16:00-17:45 PDT

---

**Title:** Election Security Bridge Building

**When:** Friday, Aug 12, 16:00 - 17:45 PDT

**Where:** Caesars Forum - Summit 224-225 - Policy Collaboratorium

**Speakers:**Jack Cable,Trevor Timmons,Michael Ross

**SpeakerBio:**Jack Cable , Congressional Fellow, Senate Homeland Security and Government Accountability Committee

No BIO available

**SpeakerBio:**Trevor Timmons

No BIO available

**SpeakerBio:**Michael Ross , Deputy Secretary of State

No BIO available

### Description:

Psst. I have heard whispers on Capitol Hill that one of the barriers to more secure elections is strengthening the trust between election workers and security researchers. And what better venue to bring together good faith researchers with election officials than DEF CON Policy?

DEF CON Policy Department is working with top election security officials and security researchers to host a roundtable discussion on strengthening trust and collaboration in election security. This session will highlight work from top researchers and members of the DEF CON community, federal government representation, and perspectives from Secretaries of State.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## DC - Sunday - 13:00-13:45 PDT

---

**Title:** ElectroVolt: Pwning popular desktop apps while uncovering new attack surface on Electron

**When:** Sunday, Aug 14, 13:00 - 13:45 PDT

**Where:** Caesars Forum - Academy 401-410, 421 (Track 3)

**Speakers:**Max Garrett,Aaditya Purani

**SpeakerBio:**Max Garrett , Application Security Auditor, Cure53

No BIO available

**SpeakerBio:**Aaditya Purani , Senior Security Engineer, Tesla

Aaditya Purani is a senior security engineer at a leading automotive company. Aaditya's primary areas of expertise are web/mobile application penetration testing, product security reviews, blockchain security, and source code review.

He contributes to responsible disclosure programs and is included in the hall of fame for Apple, Google and AT&T. He also participates in capture the flag (CTF) from perfect blue which is a globally ranked top-1 CTF team since 2020.

As a researcher, his notable public findings include BTCPay Pre-Auth RCE, Brave Browser Address Bar Vulnerability, and Akamai Zero Trust RCE. As a writer, Aaditya has authored articles for InfoSec Institute, Buzzfeed, and Hak5. In the past, Aaditya has interned for Bishop Fox and Palo Alto Networks.

Twitter: [@https://twitter.com/aaditya\\_purani](https://twitter.com/aaditya_purani)

## Description:

Electron based apps are becoming a norm these days as it allows encapsulating web applications into a desktop app which is rendered using chromium. However, if Electron apps load remote content of attackers choice either via feature or misconfiguration of Deep Link or Open redirect or XSS it would lead to Remote Code Execution on the OS.

Previously, it was known that lack of certain feature flags and inefficiency to apply best practices would cause this behavior but we have identified sophisticated novel attack vectors within the core electron framework which could be leveraged to gain remote code execution on Electron apps despite all feature flags being set correctly under certain circumstances.

This presentation covers the vulnerabilities found in twenty commonly used Electron applications and demonstrates Remote Code Execution within apps such as Discord, Teams(local file read), VSCode, Basecamp, Mattermost, Element, Notion, and others.

The speaker's would like to thank Mohan Sri Rama Krishna Pedhapati, Application Security Auditor, Cure53 and William Bowling, Senior Software Developer, Biteable for their contributions to this presentation.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## DL - Friday - 12:00-13:55 PDT

---

**Title:** EMBA - Open-Source Firmware Security Testing

**When:** Friday, Aug 12, 12:00 - 13:55 PDT

**Where:** Caesars Forum - Council Boardroom

**Speakers:**Pascal Eckmann,Michael Messner

### **SpeakerBio:**Pascal Eckmann

Pascal Eckmann: As a security researcher and developer, I have worked on several internal and Open-Source projects in the areas of fuzzing, firmware analysis and web development. In addition to automated firmware analysis, I have experience in various penetration testing areas including hardware and wireless communication.

### **SpeakerBio:**Michael Messner

Michael Messner: As a security researcher and penetration tester, I have more than 10 years of experience in different penetration testing areas. In my current position, I'm focused on hacking embedded devices used in critical environments.

## Description:

Penetration testing of current embedded devices is quite complex as we have to deal with different architectures, optimized operating systems and special protocols. EMBA is an open-source firmware analyzer with the goal to simplify, optimize and automate the complex task of firmware security analysis.

Audience: Offense (penetration testers) and defense (security team and developers).

---

## DC - Friday - 13:00-13:45 PDT

---

**Title:** Emoji Shellcoding: , , and

**When:** Friday, Aug 12, 13:00 - 13:45 PDT

**Where:** Caesars Forum - Forum 104-105, 135-136 (Track 1)

**Speakers:**Georges-Axel Jaloyan,Hadrien Barral

**SpeakerBio:**Georges-Axel Jaloyan , Hacker

Georges-Axel Jaloyan is an R&D engineer, focusing on formal methods applied to cybersecurity. He enjoys reverse-engineering and formalizing anything he comes by, always for fun and sometimes for profit.

**SpeakerBio:**Hadrien Barral , Hacker

Hadrien Barral is an R&D engineer and security expert, focusing on intrusion and high-assurance software. He enjoys hacking on exotic hardware.

### Description:

Shellcodes are short executable stubs that are used in various attack scenarios, whenever code execution is possible. After quickly recalling what a shellcode is and why designing shellcodes under constraints is an art, we'll study a new constraint for which (to the best of our knowledge) no such shellcode was previously known: emoji shellcoding. We'll tackle this problem by introducing a new and more generic approach to shellcoding under constraints. Brace yourselves, you'll see some black magic weaponizing these cute little emojis into merciless exploits .

---

## DL - Saturday - 10:00-11:55 PDT

---

**Title:** Empire 4.0 and Beyond

**When:** Saturday, Aug 13, 10:00 - 11:55 PDT

**Where:** Caesars Forum - Accord Boardroom

**Speakers:**Vincent "Vinnybod" Rose,Anthony "Cx01N" Rose

**SpeakerBio:**Vincent "Vinnybod" Rose , Lead Tool Developer

Vincent "Vinnybod" Rose is the lead developer for Empire and Starkiller. He is a software engineer with experience in cloud services, large-scale web applications, build pipeline automation, and big data ETL. 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://www.bc-security.org/blog/>.

**SpeakerBio:**Anthony "Cx01N" Rose , Lead Security Researcher

Anthony "Cx01N" Rose, CISSP, is a Security Researcher and Chief Operating Officer at BC Security, where he specializes in adversary tactic emulation planning, Red and Blue Team operations, and embedded systems security. He has presented at numerous security conferences, including Black Hat, DEF CON, and RSA conferences. Anthony is the author of various offensive security tools, including Empire and Starkiller, which he actively develops and maintains. He is recognized for his work, revealing widespread vulnerabilities in Bluetooth devices and is the co-author of a cybersecurity blog at <https://www.bc-security.org/blog/>.

Twitter: [@https://twitter.com/Cx01N\\_](https://twitter.com/Cx01N_)

## Description:

Empire is a Command and Control (C2) framework powered by Python 3 that supports Windows, Linux, and macOS exploitation. It has evolved significantly since its introduction in 2015 and has become one of the most widely used open-source C2 platforms. Starting life as PowerShell Empire and later merging in Empyre, Empire is now a full-fledged .NET C2 leveraging PowerShell, Python, C, and Dynamic Language Runtime (DLR) agents. It offers a flexible modular architecture that links Advanced Persistent Threats (APTs) Tactics, Techniques, and Procedures (TTPs) through the MITRE ATT&CK database. The framework aims to provide a flexible and easy-to-use interface to easily incorporate a wide array of tools into a single platform for red team operations to emulate APTs. This presentation will explore our most recent upgrades in Empire 4.0, including C and IronPython agents, Customizable Bypasses, Malleable HTTP C2, Donut Integration, Beacon Object File (BoF), and much more. In addition, our team will be giving a preview of Empire 5.0 and its features. The most exciting of these being the brand-new web client (Starkiller 2.0) and v2 API, which will be released later this year.

Audience: Offense

---

[Return to Index](#) - Add to



- ics [Calendar file](#)

---

## DC - Sunday - 11:00-11:45 PDT

---

**Title:** emulation-driven reverse-engineering for finding vulns

**When:** Sunday, Aug 14, 11:00 - 11:45 PDT

**Where:** Caesars Forum - Forum 106-110, 138-139 (Track 2)

**SpeakerBio:**atlas , chief pwning officer, 0fd00m c0rp0ration

atlas is a binary ninja who's been working to improve his understanding of this digital world for nearly two decades. firmware, software, hardware, rf, protocols, it's all fun to him. after all these years, he still enjoys making sense of low level things and bringing along friends who share the passion. background in development, client/server admin, hardware reversing, software reversing, vulnerability research, exploiting things in SCADA/ICS, Power Grid, Automotive, Medical, Aerospace, and devving tools to make it all easier, faster, and more consistent.

Twitter: [@https://twitter.com/atlas](https://twitter.com/atlas)

## Description:

do your eyes hurt? is your brain aching? is your pain caused from too much deciphering difficult assembly (or decompiled C) code?

assembly can hurt, C code can be worse. partial emulation to the rescue! let the emulator walk you through the code, let it answer hard questions/problems you run into in your reversing/vuln research. this talk will introduce you the power of emulator-driven reversing. guide your RE with the help of an emulator (one that can survive limited context), emulate code you don't want to reverse, be better, learn more, be faster, with less brain-drain. make no mistake, RE will always have room for magicians to show their wizardry... but after this talk, you may find yourself a much more powerful wizard.

---

[Return to Index](#) - Add to



- ics [Calendar file](#)

---

## SKY - Sunday - 09:30-10:20 PDT

---

**Title:** Eradicating Disease With BioTerrorism

**When:** Sunday, Aug 14, 09:30 - 10:20 PDT

**Where:** LINQ - BLOQ

**SpeakerBio:** Mixael S. Laufer

Mixael Swan Laufer worked in mathematics and high energy physics until he decided to use his background in science to tackle problems of global health and human rights. He continues to work to make it possible for people to manufacture their own medications and medical devices at home by creating public access to tools, ideas, and information.

Twitter: [@https://twitter.com/MichaelSLaufer](https://twitter.com/MichaelSLaufer)

**Description:**

We all know that person who never brushes their teeth, but seems never to get drilled in the dentist's chair. Why are they special? We also know the person who no matter how diligent they are with oral hygiene is constantly in the dentist's office. Why are they unlucky? The most common infectious disease in humans is dental caries, commonly referred to as cavities. This has plagued humanity since it became a species, and continues to this day. It disproportionately is suffered by those in the lower socioeconomic classes and in the global south. Conventional wisdom suggests that all that is needed is a good tooth-brushing regimen, and everything will be fine. But we know this is false. We now know that the cavity phenomenon is modulated by bacteria, and now that we can manipulate the genetic material of bacteria, we can eliminate this disease. Come see how we did it, get the new genetically modified bacteria which is the cure for yourself, and help save teeth all over the world.

---

[Return to Index](#) - Add to

[Google Calendar](#)

- ics [Calendar](#) file

---

**RHV - Saturday - 11:00-11:59 PDT**

---

**Title:** Ethical considerations in using digital footprints for verifying identities for online services

**When:** Saturday, Aug 13, 11:00 - 11:59 PDT

**Where:** Caesars Forum - Alliance 310, 320

**SpeakerBio:** Larsbodian

Larsbodian is an industrial PhD student at the Department of Computer and Systems Sciences at Stockholm University in Sweden researching IoT security integration within Enterprise Architecture.

**Description:**

Many players in the Buy Now Pay Later (BNPL) and merchant services industries are increasingly relying on digital footprint services when credit checks and national identification schemes are not easily available for different types of campaigns. There are a number of ethical considerations with this type of information gathered and used along with regulatory issues that need to be considered.

---

[Return to Index](#) - Add to

[Google Calendar](#)

- ics [Calendar](#) file

---

**WS - Saturday - 15:00-18:59 PDT**

---

**Title:** Evading Detection: A Beginner's Guide to Obfuscation

**When:** Saturday, Aug 13, 15:00 - 18:59 PDT

**Where:** Harrah's - Lake Tahoe

**Speakers:** Anthony "Cx01N" Rose, Vincent "Vinnybod" Rose, Jake "Hubbl3" Krasnov

**SpeakerBio:** Anthony "Cx01N" Rose , Lead Security Researcher

Anthony "Cx01N" Rose, CISSP, is a Security Researcher and Chief Operating Officer at BC Security, where he specializes in adversary tactic emulation planning, Red and Blue Team operations, and embedded systems security. He has presented at numerous security conferences, including Black Hat, DEF CON, and RSA conferences. Anthony is the author of various offensive security tools, including Empire and Starkiller, which he actively develops and maintains. He is recognized for his work, revealing widespread vulnerabilities in Bluetooth devices and is the co-author of a cybersecurity blog at <https://www.bc-security.org/blog/>.

Twitter: [@https://twitter.com/Cx01N\\_](https://twitter.com/Cx01N_)

### **SpeakerBio:**Vincent "Vinnybod" Rose , Lead Tool Developer

Vincent "Vinnybod" Rose is the lead developer for Empire and Starkiller. He is a software engineer with experience in cloud services, large-scale web applications, build pipeline automation, and big data ETL. 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://www.bc-security.org/blog/>.

### **SpeakerBio:**Jake "Hubbl3" Krasnov , Red Team Operations Lead and Chief Executive Officer

Jake "Hubbl3" Krasnov is the Red Team Operations Lead and Chief Executive Officer of BC Security. He has spent the first half of his career as an Astronautical Engineer overseeing rocket modifications for the Air Force. He then moved into offensive security, running operational cyber testing for fighter aircraft and operating on a red team. Jake has presented at DEF CON, where he taught courses on offensive PowerShell and has been recognized by Microsoft for his discovery of a vulnerability in AMSI. Jake has authored numerous tools, including Invoke-PrintDemon and Invoke-ZeroLogon, and is the co-author of a cybersecurity blog at <https://www.bc-security.org/blog/>.

Twitter: [@https://twitter.com/\\_Hubbl3](https://twitter.com/_Hubbl3)

### **Description:**

Defenders are constantly adapting their security to counter new threats. Our mission is to identify how they plan on securing their systems and avoid being identified as a threat. This is a hands-on class to learn the methodology behind malware delivery and avoiding detection. This workshop explores the inner workings of Microsoft's Antimalware Scan Interface (AMSI), Windows Defender, and Event Tracing for Windows (ETW). We will learn how to employ obfuscated malware using Visual Basic (VB), PowerShell, and C# to avoid Microsoft's defenses. Students will learn to build AMSI bypass techniques, obfuscate payloads from dynamic and static signature detection methods, and learn about alternative network evasion methods.

In this workshop, we will:

- i. Understand the use and employment of obfuscation in red teaming.
- ii. Demonstrate the concept of least obfuscation.
- iii. Introduce Microsoft's Antimalware Scan Interface (AMSI) and explain its importance.
- iv. Demonstrate obfuscation methodology for .NET payloads.

### Materials

Laptop VMWare or Virtual Box Windows Dev machine or other Windows VM Kali Linux VM

### Prereq

Basic level of PowerShell or C# experience.

---

[Return to Index](#) - Add to



- ics [Calendar](#) file

---

## **BTV - Saturday - 12:15-12:45 PDT**

---

**Title:** Even my Dad is a Threat Modeler!

**When:** Saturday, Aug 13, 12:15 - 12:45 PDT

**Where:** Virtual - BlueTeam Village - Talks

## **SpeakerBio:**Sarthak Taneja

Sarthak(S4T4N) is a Security Engineer passionate about everything InfoSec. He is always looking for new topics to learn. Suffering from Volunteeritis. You can always find him working with conferences behind the curtains. Right now, He is struggling to write 100 words about himself because he is habitual to writing 50 words bios.

## **Description:**

Detailed Outline will be as follows:

1. What is Threat Modelling?
2. Why is Threat Modeling necessary?
3. Common Threat Modelling Frameworks:

All the mentioned frameworks will be explained in detail with actionable scenarios and how to measure violations and propose mitigations

### **STRIDE PASTA VAST TRIKE**

3. How to plan Threat Modelling?
4. What NOT to do when doing threat modelling?
5. How to handle the results of threat modelling to not make it overwhelming to different stakeholders?

For eg:

In STRIDE, I'll give an overview and then walkthrough real life scenarios how

1. Explanantion of the framwork
2. Example: 2.1. Spoofing Identity refers to violation of authentication

Can be potrayed by misconfigured VPN configurations (in detail) 2.2 Tampering with data refers to Integrity

Having mutable logs and super admin having toxic right to change them (in detail) 2.3 Non Repudiation

Multiple users using same set of credentials causing non-repudiation and making logs useless because actions can't be backtracked to the user performing it (in details) etc

I will give examples from actual threat modellings I have done but remove all the organisation related information and make them generic, then what scenarios look like in organisations.

The talk will mainly focus on different frameworks of Threat Modelling and how threat modelling can be more efficient. Learning from the past experiences and common mistakes which organizations make while doing threat modelling.

---

[Return to Index](#) - Add to



- ics [Calendar](#) file

---

## **MIV - Friday - 11:30-13:30 PDT**

---

**Title:** Examining the urgency of gendered health misinformation online through three case studies

**When:** Friday, Aug 12, 11:30 - 13:30 PDT

**Where:** Caesars Forum - Summit 221->236

## **SpeakerBio:**Jenna Sherman

Jenna Sherman, MPH, is a Program Manager for Meedan's Digital Health Lab, an initiative focused on addressing the urgent challenges around health information equity online. She has her MPH from the Harvard T.H. Chan School of Public Health in Social and Behavioral Sciences, with a concentration in Maternal and Child Health and a focus on social epidemiology. Her work on gendered health misinformation has been featured in publications including Scientific American, The Washington

Post, and Al Jazeera.

## Description:

No Description available

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## DC - Sunday - 11:00-11:45 PDT

---

**Title:** Exploitation in the era of formal verification: a peek at a new frontier with AdaCore/SPARK

**When:** Sunday, Aug 14, 11:00 - 11:45 PDT

**Where:** Caesars Forum - Forum 104-105, 135-136 (Track 1)

**Speakers:** Adam Zabrocki, Alex Tereshkin

**SpeakerBio:** Adam Zabrocki , Principal System Software Engineer (Offensive Security) at NVIDIA

Adam Zabrocki is a computer security researcher, pentester and bughunter, currently working as a Principal Offensive Security Researcher at NVIDIA. He is a creator and developer of Linux Kernel Runtime Guard (LKRG) - his moonlight project defended by Openwall. Among others, he used to work in Microsoft, European Organization for Nuclear Research (CERN), HISPASEC Sistemas (known from the virustotal.com project), Wroclaw Center for Networking and Supercomputing, Digital. The main area of his research is low-level security (CPU arch, uCode, FW, hypervisor, kernel, OS).

As a hobby, he was a developer in The ERESI Reverse Engineering Software Interface project, a bughunter (discovered vulnerabilities in Hyper-V, KVM, RISC-V ISA, Intel's Reference Code, Intel/NVIDIA vGPU, Linux kernel, FreeBSD, OpenSSH, gcc SSP/ProPolice, Apache, Adobe Acrobat Reader, Xpdf, Torque GRID server, and more) and studied exploitation and mitigation techniques, publishing results of his research in Phrack Magazine.

Adam is driving Pointer Masking extension for RISC-V, he is a co-author of a subchapter to Windows Internals and was The Pwnie Awards 2021 nominee for most under-hyped research. He was a speaker at well-known security conferences including Blackhat, DEF CON, Security BSides, Open Source Tech conf and more.

Twitter: [@https://twitter.com/Adam\\_pi3](https://twitter.com/Adam_pi3)

**SpeakerBio:** Alex Tereshkin

Alex Tereshkin is an experienced reverse engineer and an expert in UEFI security, Windows kernel and hardware virtualization, specializing in rootkit technologies and kernel exploitation. He has been involved in the BIOS and SMM security research since 2008. He is currently working as a Principal Offensive Security Researcher at NVIDIA. He has done significant work in the field of virtualization-based malware and Windows kernel security. He is a co-author of a few courses taught at major security conferences and a co-author of the first UEFI BIOS and Intel ME exploits.

Twitter: [@https://twitter.com/AlexTereshkin](https://twitter.com/AlexTereshkin)

## Description:

For decades, software vulnerabilities have remained an unsolvable security problem regardless of years of investment in various mitigations, hardening and fuzzing strategies. In the last years there have been moves to formal methods as a path toward better security. Verification and formal methods can produce rigorous arguments about the absence of the entire classes of security bugs, and are a powerful tool to build highly secure software.

AdaCore/SPARK is a formally defined programming language intended for the development of high integrity software used in systems where predictable and highly reliable operation is crucial. The formal, unambiguous, definition of SPARK allows a variety of static analysis techniques to be applied, including information flow analysis, proof of absence of run-time exceptions, proof of termination, proof of functional correctness, and proof of safety and security properties.

In this talk we will dive-into AdaCore/SPARK, cover the blind spots and limitations, and show real-world vulnerabilities which we met during my work and which are still possible in the formally proven software. We will also show an exploit targeting one of the previously described vulnerabilities.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## DC - Saturday - 13:00-13:45 PDT

---

**Title:** Exploring Ancient Ruins to Find Modern Bugs: Discovering a 0-Day in an MS-RPC Service

**When:** Saturday, Aug 13, 13:00 - 13:45 PDT

**Where:** Caesars Forum - Academy 401-410, 421 (Track 3)

**Speakers:** Ophir Harpaz, Ben Barnea

**SpeakerBio:** Ophir Harpaz , Senior Security Research Team Lead, Akamai

Ophir Harpaz is a security research team lead in Akamai, where she manages research projects around OS internals, exploitation and malware analysis. Ophir has spoken in various security conferences including Black Hat USA, Botconf, SEC-T, HackFest and more. As an active member in Baot - a community for women engineers - she has taught a reverse-engineering workshop (<https://begin.re>) to share her enthusiasm for reversing. Ophir has entered Forbes' list of 30-under-30 and won the Rising Star category of SC Magazine's Reboot awards for her achievements and contribution to the Cyber security industry.

Twitter: [@https://twitter.com/OphirHarpaz](https://twitter.com/OphirHarpaz)

**SpeakerBio:** Ben Barnea , Senior Security Researcher, Akamai

Ben Barnea is a security researcher at Akamai with interest and experience conducting low-level security research and vulnerability research across various architectures - Windows, Linux, IoT and mobile. He likes learning how complex mechanisms work and most importantly, how they fail.

Twitter: [@https://twitter.com/nachoskrln](https://twitter.com/nachoskrln)

### Description:

MS-RPC is Microsoft's implementation of the Remote Procedure Calls protocol. Even though the protocol is extremely widespread, and serves as the basis for nearly all Windows services on both managed and unmanaged networks, little has been published about MS-RPC, its attack surface and design flaws.

In this talk, we will walkthrough and demonstrate a 0-day RCE vulnerability which we discovered through our research of MS-RPC. When exploited, this vulnerability allows an attacker to execute code remotely and potentially take over the Domain Controller. We believe this vulnerability may belong to a somewhat novel bug-class which is unique to RPC server implementations, and would like to share this idea as a possible research direction with the audience.

To aid future research into the topic of MS-RPC, we will share a deep, technical overview of the RPC system in Windows, explain why we decided to target it, and point out several design flaws. We will also outline the methodology we developed around RPC as a research target along with some tools we built to facilitate the bug-hunting process.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## DC - Friday - 15:00-15:45 PDT

---

**Title:** Exploring the hidden attack surface of OEM IoT devices: pwning thousands of routers with a vulnerability in Realtek's SDK for eCos OS.

**When:** Friday, Aug 12, 15:00 - 15:45 PDT

**Where:** Caesars Forum - Forum 104-105, 135-136 (Track 1)

**Speakers:** Octavio Galland, Octavio Gianatiempo

**SpeakerBio:** Octavio Galland , Security Researcher at Faraday

Octavio Galland is a computer science student at Universidad de Buenos Aires and a security researcher at Faraday. His main topics of interest include taking part in CTFs, fuzzing open-source software and binary reverse engineering/exploitation (mostly on x86/amd64 and MIPS).

Twitter: [@https://twitter.com/GallandOctavio](https://twitter.com/GallandOctavio)

**SpeakerBio:** Octavio Gianatiempo , Security Researcher at Faraday

Octavio Gianatiempo is a Security Researcher at Faraday and a Computer Science student at the University of Buenos Aires. He's also a biologist with research experience in molecular biology and neuroscience. The necessity of analyzing complex biological data was his point of entry into programming. But he wanted to achieve a deeper understanding of how computers work, so he enrolled in Computer Science. An entry-level CTF introduced him to the world of computer security, and there he won his first ticket to a security conference. This event was a point of no return, after which he began taking classes on computer architecture and organization and operating systems to deepen his low-level knowledge. As a Security Researcher at Faraday, he focuses on reverse engineering and fuzzing open and closed source software to find new vulnerabilities and exploit them.

Twitter: [@https://twitter.com/ogianatiempo](https://twitter.com/ogianatiempo)

**Description:**

In this presentation, we go over the main challenges we faced during our analysis of the top selling router in a local eCommerce, and how we found a zero-click remote unauthenticated RCE vulnerability. We will do a walkthrough on how we located the root cause of this vulnerability and found that it was ingrained in Realtek's implementation of a networking functionality in its SDK for eCos devices.

We then present the method we used to automate the detection of this vulnerability in other firmware images. We reflect on the fact that on most routers this functionality is not even documented and can't be disabled via the router's web interface. We take this as an example of the hidden attack surface that lurks in OEM internet-connected devices.

We conclude by discussing why this vulnerability hasn't been reported yet, despite being easy to spot (having no prior IoT experience), widespread (affecting multiple devices from different vendors), and critical.

Our research highlights the poor state of firmware security, where vulnerable code introduced down the supply chain might never get reviewed and end up having a great impact, evidencing that security is not a priority for the vendors and opening the possibility for attackers to find high impact bugs with low investment and little prior knowledge.

---

[Return to Index](#) - Add to



- ics [Calendar](#) file

---

## CPV - Saturday - 13:45-14:30 PDT

---

**Title:** Exploring Unprecedented Avenues for Data Harvesting in the Metaverse

**When:** Saturday, Aug 13, 13:45 - 14:30 PDT

**Where:** Flamingo - Vista Ballroom

**Speakers:** Gonzalo Munilla Garrido, Vivek Nair

**SpeakerBio:** Gonzalo Munilla Garrido

Gonzalo Munilla Garrido is a privacy researcher at the BMW Group and Ph.D. Student at TU Munich, where he researches privacy-enhancing technologies. His main research interests are in differential privacy and probability theory. Gonzalo has

previously been recognized as OpenMined's "contributor of the month" and has appeared in Google's "Awakening" magazine. He contributes to the security & privacy community by participating as a mentor and judge in hackathons, publishing code tutorials about differential privacy, and teaching the Blockchain Engineering course at TUM.

### **SpeakerBio:** Vivek Nair

Vivek Nair is an EECS Ph.D. student at UC Berkeley and a researcher at Cornell's IC3. As a recipient of the NSF, NPSC, and Hertz fellowships, Vivek has worked with the US Department of Defense to build resilient cyber systems. He began researching cybersecurity in 2015, when he founded Multifactor.com, and has gone on to author 12+ patents for cybersecurity technologies. He was the youngest-ever recipient of Bachelor's and Master's degrees in Computer Science at the University of Illinois at the ages of 18 and 19 respectively. Outside of cybersecurity, Vivek is a competitive VR eSports player and the captain of UC Berkeley's Beat Saber team, which he led to a US collegiate championship victory in 2021.

### **Description:**

A virtual reality (VR) user thought they were joining an anonymous server in the popular "VR Chat" application. Behind the scenes, however, an adversarial program had accurately inferred over 25 of their personal data attributes, from anthropometrics like height and wingspan to demographics like age and gender, within just a few minutes of them joining. As notoriously data-hungry companies become increasingly involved in VR development, this scenario may soon represent a typical VR user experience. While virtual telepresence applications (and the so-called "metaverse") have recently received increased attention and investment from major tech firms, these environments remain relatively under-studied from a security and privacy standpoint. In this talk, we'll illustrate via a real-time VR/XR demo how an attacker can covertly harvest personal attributes from seemingly-anonymous users of innocent-looking VR games. These attackers can be as simple as other VR users without special privilege, and the potential scale and scope of this data collection far exceed what is feasible within traditional mobile and web applications. We aim to shed light on the unique privacy risks that the metaverse entails and contribute a new way of thinking about security and privacy in emerging AR/VR environments.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## **BHV - Saturday - 10:30-10:59 PDT**

---

**Title:** Faking Positive COVID Tests

**When:** Saturday, Aug 13, 10:30 - 10:59 PDT

**Where:** Flamingo - Laughlin I,II,III

### **SpeakerBio:** Ken Gannon

Ken is a Principal Security Consultant at F-Secure who specializes in mobile security, with a hint of IoT security. He has a love/hate relationship with the medical field, as he's been involved with that field for over 10 years.

Twitter: [@https://twitter.com/Yogehi](https://twitter.com/Yogehi)

### **Description:**

I looked at 3 different COVID at-home tests this year (2 used Bluetooth, one used a camera). I tried to identify weaknesses in these tests, and with the Bluetooth specific tests I was able to fake a positive test result. In theory, my research can be used to fake a negative result as well.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## **MIV - Friday - 14:30-15:59 PDT**

---

**Title:** FARA and DOJ's Approach to Disinformation

**When:** Friday, Aug 12, 14:30 - 15:59 PDT

**Where:** Caesars Forum - Summit 221->236

**SpeakerBio:** Adam Hickey

Adam S. Hickey is a Deputy Assistant Attorney General of the National Security Division (NSD) at the Department of Justice (DOJ), overseeing the Counterintelligence and Export Control Section and the Foreign Investment Review Section. Among other things, he supervises investigations and prosecutions of foreign, state-sponsored computer intrusions and attacks, enforcement of the Foreign Agents Registration Act (FARA), and NSD's foreign investment security reviews (e.g., CFIUS work). Previously, Hickey prosecuted terrorism cases and was Deputy Chief of Appeals in the Southern District of New York. He is a graduate of Harvard College and Yale Law School.

**Description:** No Description available

[Return to Index](#) - Add to



- ics [Calendar](#) file

## ASV - Friday - 14:00-14:50 PDT

**Title:** Final Boarding Call for Cyber Policy Airlines Flight 443

**When:** Friday, Aug 12, 14:00 - 14:50 PDT

**Where:** Caesars Forum - Forum 112-117

**Speakers:** Rebecca Ash, Ayan Islam, Mary Brooks, Olivia Stella

**SpeakerBio:** Rebecca Ash

Rebecca Ash is a strategy and performance analyst with TSA's Strategy, Policy Coordination and Innovation office. In this role, she works within the TSA and interagency offices to ensure effective cybersecurity strategies to enhance the cybersecurity posture of the Transportation Systems Sector. Rebecca has a degree from George Washington University in International Affairs focusing on Latin American Studies and has been with TSA since June 2015.

**SpeakerBio:** Ayan Islam , R-Street Institute

Ayan Islam is the associate policy director of Cybersecurity and Emerging Threats at R Street Institute and adjunct lecturer of the Cyber Threats and Security policy course at American University's School of Public Affairs. Previously, she served as the critical infrastructure portfolio lead in the Insights/Mitigation team, the Operation Warp Speed liaison, and cybersecurity strategist for the Aviation Cyber Initiative (ACI) at the Cybersecurity and Infrastructure Security Agency (CISA).

**SpeakerBio:** Mary Brooks , Fellow for Cybersecurity and Emerging Threats

Mary Brooks is a fellow for Cybersecurity and Emerging Threats at the R Street Institute. Before joining R Street, she was the lead researcher and associate producer for The Perfect Weapon (2020)—an Emmy-nominated HBO documentary that explored the rise of cyber conflict as a key feature of modern inter-state competition—and was a research assistant for the book on which the film is based. She is currently a fellow in the Aspen Rising Leaders Program.

**SpeakerBio:** Olivia Stella , Senior Systems Engineer in Cybersecurity

Olivia Stella is a senior systems engineer in cybersecurity for Southwest Airlines. In her current role, she focuses on aircraft and OT cybersecurity. Her experience spans over fourteen years with a focus on the aviation, agile space, and defense systems sectors supporting incident response, vulnerability management, pen testing, bug bounty & coordinated disclosure, and risk & compliance activities.

**Description:**

Too often analysts to security researchers are left out of legislative activities. This presentation covers current affairs and the ways to get involved. We will share what has and hasn't worked, why your participation is needed, and how the collection of

cyber incident reports and statistics matters. By sharing the policy landscape, the opportunities for participation will be clear and can further efforts to build operations-policy connections. Your input is needed—don't miss your flight.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## CPV - Sunday - 11:30-11:59 PDT

---

**Title:** Finding Crypto: Inventorying Cryptographic Operations

**When:** Sunday, Aug 14, 11:30 - 11:59 PDT

**Where:** Flamingo - Vista Ballroom

### **SpeakerBio:** Kevin Lai

Kevin is a Security Engineer at Datadog in the cozy San Francisco office. After spending a decade doing full stack web development, he's moved into security for a different set of fun challenges. Out of the office you'll find him making digital art, designing games, critiquing food, and writing oddball articles.

### **Description:**

Despite the importance, most organizations don't have a good understanding of cryptographic operations in use across their various code bases. IBM's Cost of a Data Breach Report 2021 notes that organizations that use strong encryption had a \$1.25 million average lower cost of a breach than those with weak or no encryption.

Due to aging ciphers and increasing computational power, dated cipher suites are the future of insecure cryptographic practices. In order to effectively counter this threat, every organization needs to be aware of what ciphers are used, where, and how.

One solution to this problem is adding static analysis checks as part of your core continuous integration (CI) testing. In this talk, we'll see two open source static analysis solutions with default rules around detection of cryptographic weakness: Semgrep and CodeQL.

In this talk, I'll demonstrate how to implement rules with Semgrep and CodeQL, then modify cryptographic rules to suit your needs. As a demonstration, we'll look at this through the lens of achieving US Federal Information Processing Standard (FIPS) 140-2 compliance which is mandated by federal customers.

If you're looking for ways to audit, create controls, or validate tooling around determining cryptographic usage, this talk will give you solid practices to get started.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## WS - Friday - 10:00-13:59 PDT

---

**Title:** Finding Security Vulnerabilities Through Fuzzing

**When:** Friday, Aug 12, 10:00 - 13:59 PDT

**Where:** Harrah's - Elko

### **SpeakerBio:** Hardik Shah , Security Researcher

Hardik Shah is an experienced security researcher and technology evangelist. He is currently working with Sophos as a Principal Threat Researcher. Hardik has found many vulnerabilities in windows and other open source software. He currently has around 30+ CVEs in his name. He was also MSRC most valuable researcher for year 2019 and top contributing researcher

for MSRC Q1 2020. Hardik enjoys analysing latest threats and figuring out ways to protect customers from them.

You can follow him on twitter @hardik05 and read some of his blogs here: <https://news.sophos.com/en-us/author/hardik-shah/> <https://www.mcafee.com/blogs/author/hardik-shah>

Twitter: [@https://twitter.com/hardik05](https://twitter.com/hardik05)

## Description:

Many people are interested in finding vulnerabilities but don't know where to start. This workshop is aimed at providing details on how to use fuzzing to find software vulnerabilities. We will discuss what is fuzzing, different types of fuzzers and how to use them.

This training will start with a basic introduction to different types of vulnerabilities which are very common in softwares. Later on during the training we will first start with fuzzing a simple C program which contains these vulnerabilities. After that we will see how we fuzz real world open source softwares using fuzzers like AFL,libfuzzer and honggfuzz etc.

This talk will also provide details on how AFL works, what are the different mutation strategies it uses. basics of compile time instrumentation, how to collect corpus for fuzzing and how to minimize it,crash triage and finding root cause.

Key takeaways from this workshop will be: 1. Understanding of common types of security vulnerabilities like buffer overflow/heap overflow/use after free/double free/Out of bound read/write/memory leaks etc. 2. Understanding how to use various fuzzers like AFL,LibFuzzer, Hongfuzz etc. 3. How to fuzz various open source softwares on linux. 4. How to do basic debugging to find the root cause of vulnerabilities for linux. 5. How to write secure software by having an understanding of common types of vulnerabilities.

## Materials

A laptop with at least 16GB RAM, min 4 core processor, virtualbox or vmware. I will be sharing a linux VM based on kali which will have all the tools required for the workshop.

## Prereq

Basic knowledge of C,C++, basic knowledge of linux and windows.

---

[Return to Index](#) - Add to [!\[\]\(0a9aea7e63bbb8e6a746e3f7023adbaf\_img.jpg\) Google Calendar](#) - ics [Calendar file](#)

---

## MIV - Saturday - 15:15-15:45 PDT

---

**Title:** Fireside Chat

**When:** Saturday, Aug 13, 15:15 - 15:45 PDT

**Where:** Caesars Forum - Summit 221->236

**Speakers:** Arikia Millikan,Uchi Uchibeke

**SpeakerBio:** Arikia Millikan , Journalist, Media Consultant

Arikia Millikan is an American journalist and editorial strategist living in Berlin. Her journalistic work showcases my dedication to deep research and the art of the interview, bringing a humanistic perspective to topics at the intersection of technology and the human mind. In the private sector, she thrives while scrutinizing complexity and unblocking communication sticking points that occur when specialists are tasked with conveying information to a general audience. Her client roster includes founders and thought leaders from fields such as biotechnology, venture capital, telemedicine, teletherapy, femtech, cybersecurity, and mixed reality media.

**SpeakerBio:** Uchi Uchibeke

No BIO available

**Description:**No Description available

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

## MIV - Friday - 14:30-15:59 PDT

**Title:** Fireside Chat

**When:** Friday, Aug 12, 14:30 - 15:59 PDT

**Where:** Caesars Forum - Summit 221->236

**Speakers:**Adam Hickey,Jennifer Mathieu

**SpeakerBio:**Adam Hickey

Adam S. Hickey is a Deputy Assistant Attorney General of the National Security Division (NSD) at the Department of Justice (DOJ), overseeing the Counterintelligence and Export Control Section and the Foreign Investment Review Section. Among other things, he supervises investigations and prosecutions of foreign, state-sponsored computer intrusions and attacks, enforcement of the Foreign Agents Registration Act (FARA), and NSD's foreign investment security reviews (e.g., CFIUS work). Previously, Hickey prosecuted terrorism cases and was Deputy Chief of Appeals in the Southern District of New York. He is a graduate of Harvard College and Yale Law School.

**SpeakerBio:**Jennifer Mathieu

Jennifer Mathieu, PhD, is Chief Technology Officer at Graphika. She brings extensive experience building robust, integrated, cloud-based solutions to the company, enabling customers to tackle the threat of disinformation. Jennifer is responsible for guiding the company's technology vision, continuing the evolution of Graphika's patented technology, strengthening its core products, and building out the company's team of expert engineers and architects.

**Description:**No Description available

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

## DL - Friday - 10:00-11:55 PDT

**Title:** FISSURE: The RF Framework

**When:** Friday, Aug 12, 10:00 - 11:55 PDT

**Where:** Caesars Forum - Council Boardroom

**SpeakerBio:**Christopher Poore

Chris Poore is a Senior Reverse Engineer at Assured Information Security in Rome, NY. He has expertise discovering vulnerabilities in wireless systems, gaining access to systems via RF, reverse engineering RF protocols, forensically testing cybersecurity systems, and administering RF collection events. He has been the main figure behind the design and implementation of FISSURE since its inception in 2014. Chris is excited about implementing ideas drawn from the community and taking advantage of increased networking opportunities, so please reach out to him.

**Description:**

FISSURE is an open-source RF and reverse engineering framework designed for all skill levels with hooks for signal detection and classification, protocol discovery, attack execution, IQ manipulation, vulnerability analysis, automation, and AI/ML. The framework was built to promote the rapid integration of software modules, radios, protocols, signal data, scripts, flow graphs, reference material, and third-party tools. FISSURE is a workflow enabler that keeps software in one location and

allows teams to effortlessly get up to speed while sharing the same proven baseline configuration for specific Linux distributions. The framework and tools included with FISSURE are designed to detect the presence of RF energy, understand the characteristics of a signal, collect and analyze samples, develop transmit and/or injection techniques, and craft custom payloads or messages. FISSURE contains a growing library of protocol and signal information to assist in identification, packet crafting, and fuzzing. Online archive capabilities exist to download signal files and build playlists to simulate traffic and test systems.

Audience: RF, Wireless, SDR, Offense, Defense

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## CLV - Friday - 11:30-12:10 PDT

---

**Title:** Flying Under Cloud Cover: Built-in Blind Spots in Cloud Security

**When:** Friday, Aug 12, 11:30 - 12:10 PDT

**Where:** Flamingo - Scenic Ballroom

### **SpeakerBio:**Noam Dahan

Noam Dahan is a Senior Security Researcher at Ermetic with several years of experience in embedded security. He is a graduate of the Talpiot program at the Israel Defense Forces and spent several years in the 8200 Intelligence Corps. While this is his first time presenting at DEF CON, it is not his first time in front of a crowd. Noam was a competitive debater and is a former World Debating Champion.

Twitter: [@https://twitter.com/NoamDahan](https://twitter.com/NoamDahan)

### **Description:**

Every system has its blind spots. The major cloud providers are no different. The shadows in which attackers can hide out of sight (or in plain sight), and the doors that are too often left open are important parts of the cloud security landscape.

The pressure to create usability, the need to support legacy systems and workflows in a rapidly evolving landscape and the porting over of on-prem systems are just some factors that lead to these exploitable parts of cloud security.

In this talk, we'll map out a few of these built-in blind spots, focusing on AWS, Azure, and GCP in three key areas: 1) Hard knock life: Critical security areas that are hard to get right or confusingly misrepresented. 2) Trust no one! Cloud provider design flaws and backdoors that limit the degree of security that can be reached. 3) Too old for this s\*\*\*: Legacy support and dirty fixes that make for great hiding places for attackers.

We'll explore cool ways to penetrate cloud environments, escalate privilege and achieve stealth. By identifying what these weak points have in common, we can also figure out how to spot more such oversights in the future.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## ASV - Sunday - 11:30-11:55 PDT

---

**Title:** Formalizing Security Assessment for Uncrewed Aerial Systems

**When:** Sunday, Aug 14, 11:30 - 11:55 PDT

**Where:** Caesars Forum - Forum 112-117

**Speakers:**Rudy Mendoza,Ronald Broberg

## **SpeakerBio:**Rudy Mendoza , Senior Penetration Tester

Rudy Mendoza ([rudy.mendoza@darkwolfsolutions.com](mailto:rudy.mendoza@darkwolfsolutions.com)) is Senior Penetration Tester with Dark Wolf Solutions. He has been working on the Blue UAS project for the past year conducting penetration tests on multiple commercial drones for the Department of Defense. Prior to Dark Wolf Solutions he was in the U.S Air Force, where he started out as a client systems technician but quickly moved over to stand up a pathfinder program called the Mission Defense Team, providing cyber security capabilities to detect and respond to cyber threats against Air Force Space Command mission systems.

## **SpeakerBio:**Ronald Broberg

Ronald Broberg performs security assessments on Uncrewed Aerial Systems (UAS) with Dark Wolf Solutions. Previously, he was employed with Lockheed Martin. He had presented at the Aerospace Village during DEFCON 29

### **Description:**

Increased adoption of Uncrewed Aerial Systems (UAS) by a wide range of local, state, and federal government entities requires greater attention to the security requirements of UAS. Such requirements must support both operational (flight) security and data security of the UAS. We discuss the architectural decomposition used for our security assessments, common security features and failures found in current UAS, and discuss the use of IoT security frameworks in a UAS context.

---

[Return to Index](#) - Add to [!\[\]\(37239e40d8376ba31e9c79af6a892821\_img.jpg\) Google Calendar](#) - ics [Calendar file](#)

---

## **HRV - Friday - 13:00-15:59 PDT**

**Title:** Free Amateur Radio License Exams

**When:** Friday, Aug 12, 13:00 - 15:59 PDT

**Where:** Flamingo - Virginia City I

### **Description:**

Take the test to join what has been considered to be one of the first hacker communities, amateur radio! The Ham Radio Village is back at DEF CON 30 to offer free amateur radio license exams to anyone who wishes to get their ham radio license. Examinees are encouraged to study on <https://ham.study/>, and may sign up here:  
<https://ham.study/sessions/626c994a86c7aedb713d1e1f1>

---

[Return to Index](#) - Add to [!\[\]\(2d4833dc51777f63e2148563efc8aceb\_img.jpg\) Google Calendar](#) - ics [Calendar file](#)

---

## **HRV - Sunday - 11:00-13:59 PDT**

**Title:** Free Amateur Radio License Exams

**When:** Sunday, Aug 14, 11:00 - 13:59 PDT

**Where:** Flamingo - Virginia City I

### **Description:**

Take the test to join what has been considered to be one of the first hacker communities, amateur radio! The Ham Radio Village is back at DEF CON 30 to offer free amateur radio license exams to anyone who wishes to get their ham radio license. Examinees are encouraged to study on <https://ham.study/>, and may sign up here:  
<https://ham.study/sessions/626c9a8357cbff833ac7f4b7/1>

---

[Return to Index](#) - Add to [!\[\]\(fca216a1bde118e9e86df44149fba898\_img.jpg\) Google Calendar](#) - ics [Calendar file](#)

---

**Title:** Free Amateur Radio License Exams

**When:** Saturday, Aug 13, 11:00 - 16:59 PDT

**Where:** Flamingo - Virginia City I

### Description:

Take the test to join what has been considered to be one of the first hacker communities, amateur radio! The Ham Radio Village is back at DEF CON 30 to offer free amateur radio license exams to anyone who wishes to get their ham radio license. Examinees are encouraged to study on <https://ham.study/>, and may sign up here:

<https://ham.study/sessions/626c9a57d57aa149429eebf3/1>

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

## SOC - Thursday - 12:00-11:59 PDT

---

**Title:** Friends of Bill W

**When:** Thursday, Aug 11, 12:00 - 11:59 PDT

**Where:** Caesars Forum - Unity Boardroom

### Description:

For all those Friends of Bill W. looking for a meeting or just a quiet moment to regroup, we have you covered with meetings throughout #DEFCON - Noon & 5pm Thurs-Sat, Noon Sun.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

## SOC - Friday - 12:00-11:59 PDT

---

**Title:** Friends of Bill W

**When:** Friday, Aug 12, 12:00 - 11:59 PDT

**Where:** Caesars Forum - Unity Boardroom

### Description:

For all those Friends of Bill W. looking for a meeting or just a quiet moment to regroup, we have you covered with meetings throughout #DEFCON - Noon & 5pm Thurs-Sat, Noon Sun.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

## SOC - Saturday - 12:00-11:59 PDT

---

**Title:** Friends of Bill W

**When:** Saturday, Aug 13, 12:00 - 11:59 PDT

**Where:** Caesars Forum - Unity Boardroom

## Description:

For all those Friends of Bill W. looking for a meeting or just a quiet moment to regroup, we have you covered with meetings throughout #DEFCON - Noon & 5pm Thurs-Sat, Noon Sun.

---

[Return to Index](#) - Add to



- ics [Calendar](#) file

---

## SOC - Sunday - 12:00-11:59 PDT

---

**Title:** Friends of Bill W

**When:** Sunday, Aug 14, 12:00 - 11:59 PDT

**Where:** Caesars Forum - Unity Boardroom

## Description:

For all those Friends of Bill W. looking for a meeting or just a quiet moment to regroup, we have you covered with meetings throughout #DEFCON - Noon & 5pm Thurs-Sat, Noon Sun.

---

[Return to Index](#) - Add to



- ics [Calendar](#) file

---

## SOC - Saturday - 17:00-16:59 PDT

---

**Title:** Friends of Bill W

**When:** Saturday, Aug 13, 17:00 - 16:59 PDT

**Where:** Caesars Forum - Unity Boardroom

## Description:

For all those Friends of Bill W. looking for a meeting or just a quiet moment to regroup, we have you covered with meetings throughout #DEFCON - Noon & 5pm Thurs-Sat, Noon Sun.

---

[Return to Index](#) - Add to



- ics [Calendar](#) file

---

## SOC - Friday - 17:00-16:59 PDT

---

**Title:** Friends of Bill W

**When:** Friday, Aug 12, 17:00 - 16:59 PDT

**Where:** Caesars Forum - Unity Boardroom

## Description:

For all those Friends of Bill W. looking for a meeting or just a quiet moment to regroup, we have you covered with meetings throughout #DEFCON - Noon & 5pm Thurs-Sat, Noon Sun.

---

[Return to Index](#) - Add to



- ics [Calendar](#) file

---

**Title:** Friends of Bill W

**When:** Thursday, Aug 11, 17:00 - 16:59 PDT

**Where:** Caesars Forum - Unity Boardroom

## Description:

For all those Friends of Bill W. looking for a meeting or just a quiet moment to regroup, we have you covered with meetings throughout #DEFCON - Noon & 5pm Thurs-Sat, Noon Sun.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

# WS - Friday - 15:00-18:59 PDT

---

**Title:** FROM ZERO TO HERO IN A BLOCKCHAIN SECURITY

**When:** Friday, Aug 12, 15:00 - 18:59 PDT

**Where:** Harrah's - Lake Tahoe

**Speakers:**Roman Zaikin,Dikla Barda,Oded Vanunu

### **SpeakerBio:**Roman Zaikin , Security Expert

Roman Zaikin is a Security Expert. His research has revealed significant flaws in popular services, and major vendors (Facebook, WhatsApp, Telegram, eBay, AliExpress, LG, DJI, Microsoft, and more). He has over 10 years of experience in the field of cybersecurity research. He spoke at various leading conferences worldwide and taught more than 1000 students.

### **SpeakerBio:**Dikla Barda , Security Expert

Dikla Barda is a Security Expert. Her research has revealed significant flaws in popular services, and major vendors like Facebook, WhatsApp, Telegram, eBay, AliExpress, LG, DJI, Microsoft, TikTok, and more. She has over 15 years of experience in the field of cyber security research. She spoke at various leading conferences worldwide.

### **SpeakerBio:**Oded Vanunu , Head of Product Vulnerability Research

Oded Vanunu is the head of product vulnerability research and has more than 20 years of InfoSec experience, A Security Leader & Offensive Security expert.

Leading a vulnerability Research domain from a product design to product release. Issued 5 patents on cyber security defense methods. Published dozens of research papers & product CVEs.

## Description:

Blockchain technology has to be one of the biggest technology innovations of the past few years. The top emerging blockchain development trends are crypto coins, NFT, DeFi, and even metaverse. Nowadays, Companies are adopting blockchain technology and moving to the decentralized world. Especially smart contract technologies, which open them to a new cyberattack in a new crypto world. While technology evolves cybercriminals evolve along and we constantly hear about the theft of millions of dollars at security breaches in smart contracts everywhere.

In our workshop, we will teach you what is a Blockchain, what is a smart contract and what security vulnerabilities it possesses. Our workshop is intended for beginner to intermediate level hackers who want to learn new blockchain and crypto hacking techniques based on dApps TOP 10 v2022.

In the workshop, we will teach how to find vulnerabilities in blockchain smart contracts according to the latest methods and techniques. We will demonstrate every vulnerability by giving an example on the blockchain and show everything from both attacker and defender perspectives.

#### Materials

Personal Laptop

#### Prereq

Basic Programming skills in Python

---

[Return to Index](#) - Add to



- ics [Calendar](#) file

---

## HHV - Friday - 11:00-11:45 PDT

---

**Title:** From Zero To Sao ... Or, How Far Does This Rabbit Hole Go?

**When:** Friday, Aug 12, 11:00 - 11:45 PDT

**Where:** Flamingo - Exec Conf Ctr - Red Rock VI, VII, VII

#### SpeakerBio:Bradán Lane

Bradán Lane is a UX Design and User Researcher who had his own “Alice’s Adventures in Wonderland” experience when he discovered badge making. While he has made a number of fun blinky beepy ornaments and badges, he found his passion with the eChallengeCoin - an interactive and text story challenge puzzle in the shape of a coin. He releases a new eChallengeCoin each year. Bradán also designs hardware for the CircuitPython echo system so users “have a low barrier to productivity and creativity”.

#### Description:

If you have a ounce of desire and a sprinkle of creativity then you can make fun electronic tchotchkies!

You will take a journey through the software and hardware tools often used to make small electronic gadgets like DEFCON SAOs, electronic pins, and annoying blinky-beepy gifts for parties and holidays. The skills covered will also serve as the stepping off point for your own badgelife creation ... should you dare.

You will see how to take your personal strengths - be it art, maths, engineering, or fabrication - and build out to other skills.

You won’t learn everything there is to know about completing your dream project but you will have learned the steps involved and where to get help along the way!

---

[Return to Index](#) - Add to



- ics [Calendar](#) file

---

## CPV - Saturday - 10:30-10:59 PDT

---

**Title:** Fun with Factoring Large Prime Numbers

**When:** Saturday, Aug 13, 10:30 - 10:59 PDT

**Where:** Flamingo - Vista Ballroom

**Speakers:**p80n,r3c0d3

#### SpeakerBio:p80n

No BIO available

## **SpeakerBio:**r3c0d3

No BIO available

### **Description:**

Enter the world of quantum hardware, mathematical proofs, and the latest in post-quantum resistant cryptography. The quantum apocalypse is coming and it will break RSA and Diffie-Hellman. In this session, there will be a unique demo where we run code on a real quantum computer to factor “large” prime numbers using Shor’s algorithm.

[Return to Index](#) - Add to

[Google Calendar](#)

- ics [Calendar](#) file

## **AIV - Saturday - 15:00-15:50 PDT**

**Title:** Generative Art Tutorial

**When:** Saturday, Aug 13, 15:00 - 15:50 PDT

**Where:** Caesars Forum - Summit 228->236

### **Description:**

Learn how to make art with AI

[Return to Index](#) - Add to

[Google Calendar](#)

- ics [Calendar](#) file

## **HRV - Saturday - 13:00-13:30 PDT**

**Title:** Getting on the air: My experiences with Ham radio QRP

**When:** Saturday, Aug 13, 13:00 - 13:30 PDT

**Where:** Flamingo - Virginia City II

### **SpeakerBio:**Jeremy Hong

Hardware Hacker, Amateur Extra Class Ham Radio Operator (KD8TUO), Reverse Engineer at Cromulence. Featured on ARRL's QST and On The Air Publications.

<https://www.qrz.com/db/KD8TUO>

### **Description:**

Have a FCC amateur radio license or thinking about getting one? There are some easy quick ways to get on the air, and yes all it takes is some wire, balun, and a radio (this can be a raspberry pi). I'll share a few quick examples of my own.

[Return to Index](#) - Add to

[Google Calendar](#)

- ics [Calendar](#) file

## **BHV - Friday - 12:00-12:30 PDT**

**Title:** Gird your loins: premise and perils of biomanufacturing

**When:** Friday, Aug 12, 12:00 - 12:30 PDT

**Where:** Flamingo - Laughlin I,II,III

## **SpeakerBio:**Nathan Case

Successful executive and builder, pushing for change in security and the culture surrounding it. Leading strategic initiatives and the creation of new technologies in the healthcare, information technology and cloud industries, focusing on security.

Focusing on a passion for Incident Response, and operational security in all forms. Pushing the bounds of threat detection and response. Finding new thoughts and bringing them to the fields of security and technology.

## **Description:**No Description available

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## **SOC - Saturday - 20:30-23:59 PDT**

---

**Title:** Girls Hack Village 90's House Party

**When:** Saturday, Aug 13, 20:30 - 23:59 PDT

**Where:** Caesars Forum - Academy 405

### **Description:**

Nostalgia, maybe? I think so. In honor of DEF CON 30, we're throwing it back to the era of slow jams and house party mixtapes. We'll be playing everything from power ballads and rap to r&b and pop. Do like Kris Kross and Jump on the opportunity to have a good time with good people to good music.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## **SOC - Friday - 18:30-21:30 PDT**

---

**Title:** Girls Hack Village Meetup

**When:** Friday, Aug 12, 18:30 - 21:30 PDT

**Where:** Caesars Forum - Academy 409

### **Description:**

"You miss 100% of the shots you don't take" - Wayne Gretzky -Michael Scott - Girls Hack Village.

This meetup will be a fun networking event that gives attendees the opportunity to meet and make connections. Are you awkward at social gatherings? Are you the life of the party? We endeavor to create an environment where those on either side and anywhere in between are welcome and feel as though they belong. Want to grow your brand or just make new Hacker Summer Camp friends? Come one, come all.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## **DC - Friday - 12:00-12:45 PDT**

---

**Title:** Glitched on Earth by humans: A Black-Box Security Evaluation of the SpaceX Starlink User Terminal

**When:** Friday, Aug 12, 12:00 - 12:45 PDT

**Where:** Caesars Forum - Forum 104-105, 135-136 (Track 1)

## **SpeakerBio:**Lennert Wouters , researcher at imec-COSIC, KU Leuven

Lennert is a PhD researcher as the Computer Security and Industrial Cryptography (COSIC) research group, an imec research group at the KU Leuven University in Belgium. His research interests include hardware security of connected embedded devices, reverse engineering and physical attacks.

Twitter: <https://twitter.com/LennertWo>

## **Description:**

This presentation covers the first black-box hardware security evaluation of the SpaceX Starlink User Terminal (UT). The UT uses a custom quad-core Cortex-A53 System-on-Chip that implements verified boot based on the ARM trusted firmware (TF-A) project. The early stage TF-A bootloaders, and in particular the immutable ROM bootloader include custom fault injection countermeasures. Despite the black-box nature of our evaluation we were able to bypass signature verification during execution of the ROM bootloader using voltage fault injection.

Using a modified second stage bootloader we could extract the ROM bootloader and eFuse memory. Our analysis demonstrates that the fault model used during countermeasure development does not hold in practice. Our voltage fault injection attack was first performed in a laboratory setting and later implemented as a custom printed circuit board or 'modchip'. The presented attack results in an unfixable compromise of the Starlink UT and allows us to execute arbitrary code.

Obtaining root access on the Starlink UT is a prerequisite to freely explore the Starlink network and the underlying communication interfaces. This presentation will cover an initial exploration of the Starlink network. Other researchers should be able to build on our work to further explore the Starlink ecosystem.

---

[Return to Index](#) - Add to

[Google Calendar](#)

- ics [Calendar](#) file

---

## **SOC - Friday - 21:00-01:59 PDT**

---

**Title:** GOTHCON (#DCGOTHCON)

**When:** Friday, Aug 12, 21:00 - 01:59 PDT

**Where:** Caesars Forum - Forum 104-105, 136

## **Description:**

Back for their 5th year, GOTHCON welcomes everyone to come dance and stomp the night away at their Techno Coven. 9pm-2am Friday Aug 12th. Follow @dcgothcon on twitter for updates and details on location. All are welcome (except nazis), and dress however you want - whatever makes you the most comfortable and happy.

---

[Return to Index](#) - Add to

[Google Calendar](#)

- ics [Calendar](#) file

---

## **ASV - Friday - 10:00-16:59 PDT**

---

**Title:** Hack the Airfield with DDS

**When:** Friday, Aug 12, 10:00 - 16:59 PDT

**Where:** Caesars Forum - Forum 112-117

## **Description:**

Hack the Airfield is broken down into two primary components, the aircraft and the system used to locate and find them.

## **BRICKS IN THE AIR**

Learn how avionics systems work in a safe and fun way in our Bricks in the Air workshop that simulates an environment

requiring similar approaches to hacking on actual aviation buses without using any of the real hardware, protocols, or commands. Challengers can freely play and develop skills without worrying about legalities or sensitivities of real systems.

## SPOOFING ADS-B

ADS-B is the latest version of Identify Friend or Foe (IFF), which is the common name for cooperative radar surveillance of aircraft. Unlike traditional IFF, in ADS-B the aircraft periodically sends a broadcast out roughly every half second to alert all nearby receivers of its current location. These broadcasts are unencrypted and fairly easy to spoof, allowing anyone to create as many aircraft as they want. Stop by the workshop and learn what it takes to spoof fake aircraft into the system used to track them.

Required gear: none!

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## ASV - Sunday - 10:00-12:59 PDT

---

**Title:** Hack the Airfield with DDS

**When:** Sunday, Aug 14, 10:00 - 12:59 PDT

**Where:** Caesars Forum - Forum 112-117

### Description:

Hack the Airfield is broken down into two primary components, the aircraft and the system used to locate and find them.

## BRICKS IN THE AIR

Learn how avionics systems work in a safe and fun way in our Bricks in the Air workshop that simulates an environment requiring similar approaches to hacking on actual aviation buses without using any of the real hardware, protocols, or commands. Challengers can freely play and develop skills without worrying about legalities or sensitivities of real systems.

## SPOOFING ADS-B

ADS-B is the latest version of Identify Friend or Foe (IFF), which is the common name for cooperative radar surveillance of aircraft. Unlike traditional IFF, in ADS-B the aircraft periodically sends a broadcast out roughly every half second to alert all nearby receivers of its current location. These broadcasts are unencrypted and fairly easy to spoof, allowing anyone to create as many aircraft as they want. Stop by the workshop and learn what it takes to spoof fake aircraft into the system used to track them.

Required gear: none!

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## ASV - Saturday - 10:00-16:59 PDT

---

**Title:** Hack the Airfield with DDS

**When:** Saturday, Aug 13, 10:00 - 16:59 PDT

**Where:** Caesars Forum - Forum 112-117

### Description:

Hack the Airfield is broken down into two primary components, the aircraft and the system used to locate and find them.

## **BRICKS IN THE AIR**

Learn how avionics systems work in a safe and fun way in our Bricks in the Air workshop that simulates an environment requiring similar approaches to hacking on actual aviation buses without using any of the real hardware, protocols, or commands. Challengers can freely play and develop skills without worrying about legalities or sensitivities of real systems.

### **SPOOFING ADS-B**

ADS-B is the latest version of Identify Friend or Foe (IFF), which is the common name for cooperative radar surveillance of aircraft. Unlike traditional IFF, in ADS-B the aircraft periodically sends a broadcast out roughly every half second to alert all nearby receivers of its current location. These broadcasts are unencrypted and fairly easy to spoof, allowing anyone to create as many aircraft as they want. Stop by the workshop and learn what it takes to spoof fake aircraft into the system used to track them.

Required gear: none!

---

[Return to Index](#) - Add to [!\[\]\(191da1b4ad6c7d8c17d24a21911feb83\_img.jpg\) Google Calendar](#) - ics [Calendar](#) file

---

## **ASV - Saturday - 10:00-16:59 PDT**

---

**Title:** Hack the Airport with Intelligenesis

**When:** Saturday, Aug 13, 10:00 - 16:59 PDT

**Where:** Caesars Forum - Forum 112-117

### **Description:**

Can you restore the Aerospace Village runway lighting system? IntelliGenesis will be holding a mini-Hack the Airport that is designed to showcase the impact of a cyber-attack on critical infrastructure commercial or government facilities; specifically, Aviation Control Systems. Transportation Systems is one of the 16 Cybersecurity and Infrastructure Agency Critical Infrastructure Sectors for the US. There is a hyper focus on cybersecurity surrounding airports and the critical infrastructure systems supporting aviation operations. Come on over and give it an attempt, there will be 4 stages culminating in restoring the lighting system so that the village can begin landing and launching aircraft. All levels of experience can participate.

Signups: beginning Monday 8/8 – but not required to participate

---

[Return to Index](#) - Add to [!\[\]\(e606f31a15d3dd682e4fb1cca194bc0a\_img.jpg\) Google Calendar](#) - ics [Calendar](#) file

---

## **ASV - Friday - 10:00-16:59 PDT**

---

**Title:** Hack the Airport with Intelligenesis

**When:** Friday, Aug 12, 10:00 - 16:59 PDT

**Where:** Caesars Forum - Forum 112-117

### **Description:**

Can you restore the Aerospace Village runway lighting system? IntelliGenesis will be holding a mini-Hack the Airport that is designed to showcase the impact of a cyber-attack on critical infrastructure commercial or government facilities; specifically, Aviation Control Systems. Transportation Systems is one of the 16 Cybersecurity and Infrastructure Agency Critical Infrastructure Sectors for the US. There is a hyper focus on cybersecurity surrounding airports and the critical infrastructure systems supporting aviation operations. Come on over and give it an attempt, there will be 4 stages culminating in restoring the lighting system so that the village can begin landing and launching aircraft. All levels of experience can participate.

Signups: beginning Monday 8/8 – but not required to participate

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## ASV - Sunday - 10:00-12:59 PDT

---

**Title:** Hack the Airport with Intelligenesis

**When:** Sunday, Aug 14, 10:00 - 12:59 PDT

**Where:** Caesars Forum - Forum 112-117

### Description:

Can you restore the Aerospace Village runway lighting system? IntelliGenesis will be holding a mini-Hack the Airport that is designed to showcase the impact of a cyber-attack on critical infrastructure commercial or government facilities; specifically, Aviation Control Systems. Transportation Systems is one of the 16 Cybersecurity and Infrastructure Agency Critical Infrastructure Sectors for the US. There is a hyper focus on cybersecurity surrounding airports and the critical infrastructure systems supporting aviation operations. Come on over and give it an attempt, there will be 4 stages culminating in restoring the lighting system so that the village can begin landing and launching aircraft. All levels of experience can participate.

Signups: beginning Monday 8/8 – but not required to participate

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## DC - Saturday - 13:30-14:15 PDT

---

**Title:** HACK THE HEMISPHERE! How we (legally) broadcasted hacker content to all of North America using an end-of-life geostationary satellite, and how you can set up your own broadcast too!

**When:** Saturday, Aug 13, 13:30 - 14:15 PDT

**Where:** Caesars Forum - Forum 106-110, 138-139 (Track 2)

**Speakers:** Andrew Green, Karl Koscher

### SpeakerBio: Andrew Green , Hacker

Andrew Green is a multidisciplinary jack of all trades, who specializes in information technology and broadcasting. He brings together many years of unique experiences, with a talent for understanding complex systems on the fly. He currently holds an Advanced amateur radio license, VO1VO.

### SpeakerBio: Karl Koscher , Hacker

Karl Koscher is a technology and security generalist with an emphasis on wireless and embedded systems security. As part of his dissertation work at the University of Washington, he and his collaborators were the first to demonstrate a complete remote compromise of a car over cellular, Bluetooth and other channels. He is a co-organizer of the Crypto and Privacy Village and holds an Amateur Extra license.

### Description:

The Shadytel cabal had an unprecedented opportunity to legally uplink to and use a vacant transponder slot on a geostationary satellite about to be decommissioned. This talk will explain how we modified an unused commercial uplink facility to broadcast modern HD DVB-S2 signals and created the media processing chain to generate the ultimate information broadcast. You'll learn how satellite transponders work, how HDTV is encoded and transmitted, and how you can create your own hacker event broadcast.

## ASV - Saturday - 12:00-16:59 PDT

---

**Title:** Hack-A-Sat Aerospace PiSat Challenge

**When:** Saturday, Aug 13, 12:00 - 16:59 PDT

**Where:** Caesars Forum - Forum 112-117

### Description:

Engineers at the Aerospace Corporation are hosting a CTF using the PiSat platform (check out the PiSat Workshop also in the Aerospace Village). Teams will command a PiSat via a COSMOS web GUI and complete challenges, which will be announced during the event. The CTF will primarily use crosslinks between PiSats to complete tasks including attacking other PiSats. Rounds will last ten minutes each, but teams can stay for up to one hour.

Required gear: bring a laptop (with an ethernet port!) to compete in the contest.

Signups: Sign-ups for the event will be in person each morning from 10am – 12pm and will be first come, first served.

---

## ASV - Friday - 12:00-16:59 PDT

---

**Title:** Hack-A-Sat Aerospace PiSat Challenge

**When:** Friday, Aug 12, 12:00 - 16:59 PDT

**Where:** Caesars Forum - Forum 112-117

### Description:

Engineers at the Aerospace Corporation are hosting a CTF using the PiSat platform (check out the PiSat Workshop also in the Aerospace Village). Teams will command a PiSat via a COSMOS web GUI and complete challenges, which will be announced during the event. The CTF will primarily use crosslinks between PiSats to complete tasks including attacking other PiSats. Rounds will last ten minutes each, but teams can stay for up to one hour.

Required gear: bring a laptop (with an ethernet port!) to compete in the contest.

Signups: Sign-ups for the event will be in person each morning from 10am – 12pm and will be first come, first served.

---

## ASV - Sunday - 10:00-12:59 PDT

---

**Title:** Hack-A-Sat Digital Twin Workshop

**When:** Sunday, Aug 14, 10:00 - 12:59 PDT

**Where:** Caesars Forum - Forum 112-117

## Description:

The Hack-A-Sat team is working hard to build the next competition platform for the Hack-A-Sat 3 (HAS3) Finals competition, where space math, hacking, and satellite operations are interwoven into a realistic space CTF environment. We will be demoing the HAS3 digital twin satellite in the Aerospace Village for participants to experience basic satellite command & control operations and flight software exploitation with two challenges created specifically for DEF CON. This year's digital twin brings new tools, processor architecture, and physics simulation capabilities that we will be unveiling for the first time.

Required gear: We are hosting the demo on our own hardware so all you need to bring is your own desire to "Learn. Space. Faster".

Signups: first come first serve, come by the Aerospace Village during its normal operating hours!

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## ASV - Friday - 10:00-16:59 PDT

---

**Title:** Hack-A-Sat Digital Twin Workshop

**When:** Friday, Aug 12, 10:00 - 16:59 PDT

**Where:** Caesars Forum - Forum 112-117

### Description:

The Hack-A-Sat team is working hard to build the next competition platform for the Hack-A-Sat 3 (HAS3) Finals competition, where space math, hacking, and satellite operations are interwoven into a realistic space CTF environment. We will be demoing the HAS3 digital twin satellite in the Aerospace Village for participants to experience basic satellite command & control operations and flight software exploitation with two challenges created specifically for DEF CON. This year's digital twin brings new tools, processor architecture, and physics simulation capabilities that we will be unveiling for the first time.

Required gear: We are hosting the demo on our own hardware so all you need to bring is your own desire to "Learn. Space. Faster".

Signups: first come first serve, come by the Aerospace Village during its normal operating hours!

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## ASV - Saturday - 10:00-16:59 PDT

---

**Title:** Hack-A-Sat Digital Twin Workshop

**When:** Saturday, Aug 13, 10:00 - 16:59 PDT

**Where:** Caesars Forum - Forum 112-117

### Description:

The Hack-A-Sat team is working hard to build the next competition platform for the Hack-A-Sat 3 (HAS3) Finals competition, where space math, hacking, and satellite operations are interwoven into a realistic space CTF environment. We will be demoing the HAS3 digital twin satellite in the Aerospace Village for participants to experience basic satellite command & control operations and flight software exploitation with two challenges created specifically for DEF CON. This year's digital twin brings new tools, processor architecture, and physics simulation capabilities that we will be unveiling for the first time.

the first time.

Required gear: We are hosting the demo on our own hardware so all you need to bring is your own desire to “Learn. Space. Faster”.

Signups: first come first serve, come by the Aerospace Village during its normal operating hours!

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## ASV - Friday - 10:00-10:50 PDT

---

**Title:** Hack-A-Sat Team

**When:** Friday, Aug 12, 10:00 - 10:50 PDT

**Where:** Caesars Forum - Forum 112-117

### Description:

Hack-A-Sat (HAS) is an Air Force/Space Force satellite hacking CTF, now in its 3rd year. This talk will: 1) educate the audience on the HAS series of competitions, 2) review challenges/solves from the HAS3 qualifiers in May 2022, 3) preview the HAS3 Finals (Oct 2022) including the 8 finalist teams vying for \$100K prize pool, 4) talk about Moonlighter, a cubesat designed and built as a hacking sandbox in space. Moonlighter will be the platform for HAS4, the world’s first CTF in space.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## SOC - Saturday - 20:00-21:59 PDT

---

**Title:** Hacker Flairgrounds

**When:** Saturday, Aug 13, 20:00 - 21:59 PDT

**Where:** Caesars Forum - Accord Boardroom

### Description:

The destination for badge collectors, designers, and hardware hacks to celebrate the flashier side of DEF CON. It is a melding of the 1337 and the unleet interested in hardware and IoT. We see #badgelife, #badgelove, SAOs and badge hacking as a great potential for securing IoT and keeping the power in the hands of the consumer by spreading knowledge about the craft/trade. Those involved should be celebrated for sharing their knowledge. Many of them do not like the limelight, so this gives us a chance to personally say thank you in a chill environment.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## SOC - Friday - 20:00-21:59 PDT

---

**Title:** Hacker Jeopardy

**When:** Friday, Aug 12, 20:00 - 21:59 PDT

**Where:** Caesars Forum - Alliance 301-309, 321 (Track 4)

## Description:

Hacker Jeopardy, the classic DEF CON game show, is returning for yet another year of answers, questions, NULL beers, and occasionally some impressive feats of knowledge. You don't want to miss this opportunity to encourage the contestants, your fellow Humans, "DON'T FUCK IT UP!"

We will be opening auditions, with the call posted on the dfiu.tv website, and linked to DEF CON forums. (promoted on social media)

Track 4

Friday: 2000-2200

Saturday: 2000-2200

---

[Return to Index](#) - Add to



- ics [Calendar](#) file

---

## **SOC - Saturday - 20:00-21:59 PDT**

---

**Title:** Hacker Jeopardy

**When:** Saturday, Aug 13, 20:00 - 21:59 PDT

**Where:** Caesars Forum - Alliance 301-309, 321 (Track 4)

## Description:

Hacker Jeopardy, the classic DEF CON game show, is returning for yet another year of answers, questions, NULL beers, and occasionally some impressive feats of knowledge. You don't want to miss this opportunity to encourage the contestants, your fellow Humans, "DON'T FUCK IT UP!"

We will be opening auditions, with the call posted on the dfiu.tv website, and linked to DEF CON forums. (promoted on social media)

Track 4

Friday: 2000-2200

Saturday: 2000-2200

---

[Return to Index](#) - Add to



- ics [Calendar](#) file

---

## **SOC - Saturday - 19:30-01:59 PDT**

---

**Title:** Hacker Karaoke

**When:** Saturday, Aug 13, 19:30 - 01:59 PDT

**Where:** Caesars Forum - Forum 133

## Description:

For those who love to sing and perform in front of others, we are celebrating our 14th year of Love, Laughter, and Song from 8 PM to 2 AM Friday and Saturday night.

We are open to everyone of any age, and singing is not required.

For more information visit:

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

## SOC - Friday - 19:30-01:59 PDT

**Title:** Hacker Karaoke

**When:** Friday, Aug 12, 19:30 - 01:59 PDT

**Where:** Caesars Forum - Forum 133

### Description:

For those who love to sing and perform in front of others, we are celebrating our 14th year of Love, Laughter, and Song from 8 PM to 2 AM Friday and Saturday night.

We are open to everyone of any age, and singing is not required.

For more information visit:

<https://hackerkaraoke.org> or Twitter @hackerkaraoke.

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

## ASV - Friday - 12:00-12:50 PDT

**Title:** Hackers Help Make My Airline Secure

**When:** Friday, Aug 12, 12:00 - 12:50 PDT

**Where:** Caesars Forum - Forum 112-117

### SpeakerBio:

Deneen Defiore

Deneen is an accomplished technology & risk management executive with experience across multiple critical infrastructure sectors. She has expertise in advising global companies & their most senior executives on technology, cybersecurity, compliance, and digital risk related decisions associated to products, services, significant initiatives, & ongoing operations. Deneen currently serves as Vice President and Chief Information Security Officer at United Airlines. She is responsible for leading the cybersecurity organization to ensure the company is prepared to prevent, detect, & respond to evolving cyber threats; as well as commercial aviation cyber safety risk initiatives & improving cyber resilience across the global aviation ecosystem.

### Description:

Ensuring passengers are safe while flying goes well beyond the cybersecurity of just an aircraft. Join this fireside chat with Deneen DeFiore, the Chief Information Security Officer for United Airlines, to learn how she is building an enterprise security program that leverages smart, experienced hackers. Deneen will share her background in infosec along with her approach to engaging security expertise to maintain the trust her customers have in her airline's safe and secure operations.

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

**Title:** Hacking Aviation Policy

**When:** Saturday, Aug 13, 12:00 - 13:45 PDT

**Where:** Caesars Forum - Summit 224-225 - Policy Collaboratorium

**Speakers:** Timothy Weston, Ayan Islam, Meg King, Ken Munro, Pete Cooper

**SpeakerBio:** Timothy Weston , Deputy Executive Director (acting), Cybersecurity Policy Coordinator, Transportation Security Administration

Tim Weston is the Director for Strategy & Performance in TSA's office of Strategy, Policy Coordination and Innovation. Mr. Weston also serves as the TSA Cybersecurity Policy Coordinator. Previously, he worked in the TSA Office of Chief Counsel, as Senior Counsel in the Security Threat Assessment Division.

**SpeakerBio:** Ayan Islam , R-Street Institute

Ayan Islam is the associate policy director of Cybersecurity and Emerging Threats at R Street Institute and adjunct lecturer of the Cyber Threats and Security policy course at American University's School of Public Affairs. Previously, she served as the critical infrastructure portfolio lead in the Insights/Mitigation team, the Operation Warp Speed liaison, and cybersecurity strategist for the Aviation Cyber Initiative (ACI) at the Cybersecurity and Infrastructure Security Agency (CISA).

**SpeakerBio:** Meg King , Executive Director for Strategy, Policy Coordination & Innovation, Transportation Security Administration

No BIO available

**SpeakerBio:** Ken Munro , Pentest Partners

Ken Munro is Partner and Founder of Pen Test Partners, a firm of penetration testers with a keen interest in aviation. Pen Test Partners has several pilots on the team, both private and commercial, recognizing that the increase in retired airframes has created opportunities for independent security research into aviation security. Pen Test Partners has been recognized for its highly responsible approach to vulnerability disclosure in aviation and was invited to join the Boeing Cyber Technical Council as a result. Pen Test Partners has published research into aviation cyber security, covering topics from airborne connectivity, avionics hardware, and connectivity with ground systems.

**SpeakerBio:** Pete Cooper , Deputy Director Cyber Defence, Cabinet Office

No BIO available

### Description:

TSA and DEFCON will host a policy discussion group focused on the current cybersecurity threats to the aviation ecosystem. Discussion will be focused on the increasing threat space focused on airports, airframes, airlines, and air cargo. Additional topics of discussion will focus on cybersecurity work force issues, prioritization of mitigation measures to counter the threats, and how the research community can assist the government and the private sector. The aviation sector policy discussion will be held under Chatham House rules, otherwise known as "what happens in Vegas, stays in Vegas," with the desired outcome that participants will come away with a better understanding of the threats, possible solutions, and the importance of collaboration to solve these pressing issues. Given the global nature of aviation, we will touch on the partnerships and policy regimes under consideration by the international community.

---

[Return to Index](#) - Add to



- ics [Calendar](#) file

**When:** Friday, Aug 12, 15:00 - 15:59 PDT

**Where:** Flamingo - Virginia City II

### **SpeakerBio:**Rick Osgood

Rick has been an enthusiastic penetration tester since 2015, and has been involved with the security community since 2005. As a Principal Security Consultant at Coalfire, Rick conducts application and API tests, cloud testing, network penetration tests, and wireless tests. He has also completed multiple security-related research and development projects.

Rick dove into information security in 2005, enrolling in a university program specifically designed around network security. He has experience as a Linux system engineer, security analyst, and penetration tester. Rick has volunteered at both Blackhat and Defcon, and co-founded two non-profit hackerspaces: HeatSync Labs in Arizona, and Eugene Maker Space in Oregon. Rick interests include radio and electronics, which are sometimes combined with security projects. He has also written for the popular security-related blog [hackaday.com](http://hackaday.com).

Twitter: <https://twitter.com/rickoooooooo>

<https://www.richardosgood.com>

### **Description:**

Amateur radio can be used to communicate with operators all over the world using voice, Morse code, or even computers. When connected to a computer, our rigs can do anything from text messaging and email to sharing images and tracking weather balloons. There's something magical about connecting to a device or person across the planet without the modern Internet, but can these connections be abused? Of course, they can! This presentation will review a memory corruption exploit developed to obtain remote code execution via ham radio. The presentation will briefly describe packet radio and APRS before moving on to target selection, fuzzing, reverse engineering, shellcode development, and exploitation. Prior understanding of basic exploit techniques such as simple buffer overflows and SEH overwrites is helpful, but not strictly required.

[Return to Index](#) - Add to



- ics [Calendar](#) file

## PWV - Friday - 13:00-12:59 PDT

**Title:** Hacking Hashcat

**When:** Friday, Aug 12, 13:00 - 12:59 PDT

**Where:** Caesars Forum - Summit 218-219

**SpeakerBio:**Ray "Senpai" Morris

No BIO available

### **Description:**

Cracking Passwords to Make Them Strong

Existing password meters say that passwords like ""Fall2021!"" or ""Password123!"" are strong, just because they have upper case, lower case, and numbers. ""Password123!"" is NOT a strong password; it will get cracked in seconds. I gave 47,000 "strong" password hashes to some of the best password crackers. Although the meters said these passwords were strong, over 99% of them actually got cracked.

By reversing the tools the password crackers *actually* use, we can tell whether a password will actually be cracked, by real password crackers, including those who win the Defcon Crack Me If You Can.

I will demonstrate a new open source Python tool which tells you with over 90% accuracy whether a real password cracker

would be able to crack the password you're thinking about using. This tool tests the types of attacks that crackers conduct using tools like Hashcat or John the Ripper.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## DC - Friday - 16:00-16:45 PDT

---

**Title:** Hacking ISPs with Point-to-Pwn Protocol over Ethernet (PPPoE)

**When:** Friday, Aug 12, 16:00 - 16:45 PDT

**Where:** Caesars Forum - Forum 104-105, 135-136 (Track 1)

**SpeakerBio:** Gal Zror , Vulnerability Research Manager at CyberArk Labs

Gal Zror (@waveburst) acts as the vulnerability research manager in CyberArk labs. Gal has over 12 years of experience in vulnerability research and he specializes in embedded systems and protocols. Besides research, he is also an amateur boxer and a tiki culture enthusiast.

Twitter: [@https://twitter.com/waveburst](https://twitter.com/waveburst)

### Description:

Hello, my name is BWL-X8620, and I'm a SOHO router. For many years my fellow SOHO routers and I were victims of endless abuse by hackers. Default credentials, command injections, file uploading - you name it. And it is all just because we're WAN-facing devices. Just because our ISP leaves our web server internet-facing makes hackers think it's okay to attack and make us zombies. But today, I say NO MORE!

In this talk, I will show that if a web client can attack a web server, then an ISP client can attack the ISP servers! I will reveal a hidden attack surface and vulnerabilities in popular network equipment used by ISPs worldwide to connect end-users to the internet. BRAS devices are not that different from us SOHO routers. No one is infallible. But, BRAS devices can support up to 256,000 subscribers, and exploiting them can cause a ruckus. Code executing can lead to a total ISP compromise, mass client DNS poisoning, end-points RCE, and more!

This talk will present a high severity logical DOS vulnerability in a telecommunications vendor implementation of PPPoE and a critical RCE vulnerability in PPP. That means we, the SOHO routers, can attack and execute code on the ISP's that connect us to the internet!

Today we are fighting back!

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## PLV - Friday - 12:00-13:45 PDT

---

**Title:** Hacking law is for hackers - how recent changes to CFAA, DMCA, and global policies affect security research

**When:** Friday, Aug 12, 12:00 - 13:45 PDT

**Where:** Caesars Forum - Summit 226-227 - Policy Roundtable

**Speakers:** Leonard Bailey, Harley Geiger

**SpeakerBio:** Leonard Bailey , Head of the Cybersecurity Unit and Special Counsel for National Security

No BIO available

**SpeakerBio:** Harley Geiger , Senior Director for Public Policy

No BIO available

## Description:

What a year for hacker law! 2021-2022 saw major changes to laws that regulate hacking, such as the notorious CFAA, the grotesque DMCA Sec. 1201, and China's grisly "Management of Security Vulnerabilities" regulation. This presentation will walk through each of these developments and detail their implications for security researchers. We'll give background on how these laws have recently changed, identify areas of continued risk for hackers, and suggest concrete ways for the security community to make additional progress in shaping a favorable legal environment. An extended roundtable discussion will follow the presentation.

[Return to Index](#) - Add to



- ics [Calendar file](#)

## PLV - Saturday - 10:00-11:45 PDT

**Title:** Hacking Operational Collaboration

**When:** Saturday, Aug 13, 10:00 - 11:45 PDT

**Where:** Caesars Forum - Summit 224-225 - Policy Collaboratorium

**SpeakerBio:**David Forscay

No BIO available

## Description:

CISA/JCDC leadership will speak on a panel to review the purpose and history of JCDC, and set the scene for the event before attendees begin their own conversations. Following the panel, attendees will split up into four breakout sections and gather in four corners of the room. Each of these groups will divide again to form no more than 5-6 people per discussion group. These small groups will delve into one proposal for a JCDC initiative and discuss for 15-20 minutes, after which they will rotate to the next section/topic. Each conversation will be facilitated by CISA, who play the “champion” for that specific proposal. Topics may include: Transnational Trust Webs (How can JCDC collaborate with researchers, orgs, and partners spread across the globe? Internet security, not just national security); Chaos Engine (How do we turn the Internet into a much more risky place for adversaries? Which hackers have the right data to find adversary infrastructure?); We Want You (How can CISA expand on its past work with individuals on research to integrate volunteer hackers into response operations?); Expect the Worst (What kind of contingencies should CISA prioritize? What planning and preparation can achieve the most leverage if the worst happens?)

[Return to Index](#) - Add to



- ics [Calendar file](#)

## IOTV - Friday - 11:30-11:59 PDT

**Title:** Hacking Product Security Interviews

**When:** Friday, Aug 12, 11:30 - 11:59 PDT

**Where:** Caesars Forum - Alliance 311, 320

## Description:

Hacking Product Security Interviews

Cybersecurity is a complex, multi-faceted field and pursuing a career in it requires the acquisition of a number of different skill sets. Product Security interviews can be particularly challenging due to the expectation that candidates possess both hacking AND software engineering intuition and skills.

Zoox will take a software engineering perspective and unpack this topic in an interactive talk. They focus on big-picture as well as tactical insights that will help you invest your time when preparing for your dream Product Security job. This is an interactive group activity!

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## IOTV - Friday - 11:00-11:30 PDT

---

**Title:** Hacking Product Security Interviews

**When:** Friday, Aug 12, 11:00 - 11:30 PDT

**Where:** Caesars Forum - Alliance 311, 320

### Description:

Hacking Product Security Interviews

Cybersecurity is a complex, multi-faceted field and pursuing a career in it requires the acquisition of a number of different skill sets. Product Security interviews can be particularly challenging due to the expectation that candidates possess both hacking AND software engineering intuition and skills.

Zoox will take a software engineering perspective and unpack this topic in an interactive talk. They focus on big-picture as well as tactical insights that will help you invest your time when preparing for your dream Product Security job. This is an interactive group activity!

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## DC - Saturday - 17:00-17:45 PDT

---

**Title:** Hacking The Farm: Breaking Badly Into Agricultural Devices.

**When:** Saturday, Aug 13, 17:00 - 17:45 PDT

**Where:** Caesars Forum - Forum 104-105, 135-136 (Track 1)

### SpeakerBio:

Sick Codes , Hacker  
Ordinary everyday hacker.

Sick Codes is an alleged Australian hacker, who resides somewhere in Asia: I love finding vulns, the thrill of the the 0day, emulation, free software, reverse engineering, standing up for other researchers & fast motorbikes. I hack anything with an electromagnetic pulse, including TV's, cars, tractors, ice cream machines, and more. My heart lies with Free Software but I like to go where no researcher has gone before. My works include Docker-OSX, which regularly trends on GitHub with 22k+ stars, 300k+ downloads.

Twitter: [@https://twitter.com/sickcodes](https://twitter.com/sickcodes)

### Description:

Hacking the farm. In this session, I'll demonstrate tractor-sized hardware hacking techniques, firmware extraction, duplication, emulation, and cloning. We'll be diving into how the inner workings of agricultural cyber security; how such low-tech devices are now high-tech devices. The "connected farm" is now a reality; a slurry of EOL devices, trade secrets, data transfer, and overall shenanigans in an industry that accounts for roughly one-fifth of the US economic activity. We'll be discussing hacking into tractors, combines, cotton harvesters, sugar cane and more.

---

## WS - Friday - 15:00-18:59 PDT

---

**Title:** Hacking the Metal 2: Hardware and the Evolution of C Creatures

**When:** Friday, Aug 12, 15:00 - 18:59 PDT

**Where:** Harrah's - Copper

**SpeakerBio:**Eigentourist , Programmer

Eigentourist is a programmer who learned the craft in the early 1980s. He began formal education in computer science when the height of software engineering discipline meant avoiding the use of GOTO statements. Over the course of his career, he has created code of beautiful simplicity and elegance, and of horrific complexity and unpredictability. Sometimes it's hard to tell which was which. Today, he works on systems integration and engineering in the healthcare industry.

### Description:

Beneath the surface of your favorite video game, operating system, or mobile app hides a subterranean world of low-level programming and hardware architecture that was once the domain of all programmers, but now lives mostly hidden behind dazzling graphics and modern abstractions. Diving into this world, we will delve into the design of processors using a hardware description language, tour through a handful of assembly language programs, and then plunge into systems programming in C, with comparison and contrast to the underlying assembly language that the compiler generates. Along the way, we will build programs both entertaining and mischievous, and emerge with a deeper understanding of the secrets behind all modern digital computing.

Materials

Laptop

Prereq

Some coding experience is helpful but not mandatory

---

## SOC - Friday - 21:00-01:59 PDT

---

**Title:** Hallway Monitor Party - Entertainment

**When:** Friday, Aug 12, 21:00 - 01:59 PDT

**Where:** Caesars Forum - Skybridge Entrance

**Speakers:**DJ UNIT 77 [ 0077 : 0077 ],CaptHz,DJ Scythe,Magik Plan,Tense Future

**SpeakerBio:**DJ UNIT 77 [ 0077 : 0077 ]

No BIO available

**SpeakerBio:**CaptHz

No BIO available

**SpeakerBio:**DJ Scythe

No BIO available

**SpeakerBio:**Magik Plan

No BIO available

### **SpeakerBio:**Tense Future

No BIO available

#### **Description:**

21:00 - 22:00: Tense Future

22:00 - 23:00: DJ Scythe

**23:00 - 00:00: DJ UNIT 77 [ 0077 : 0077 ]** 00:00 - 01:00: CaptHz

01:00 - 02:00: Magik Plan

---

[Return to Index](#) - Add to [!\[\]\(abf8628d4ace9a335e814b1472adea7b\_img.jpg\) Google Calendar](#) - ics [Calendar](#) file

---

## **SOC - Saturday - 21:00-01:59 PDT**

---

**Title:** Hallway Monitor Party - Entertainment

**When:** Saturday, Aug 13, 21:00 - 01:59 PDT

**Where:** Caesars Forum - Skybridge Entrance

**Speakers:**Yesterday & Tomorrow,Terrestrial Access Network,Hellacopta,Hanz Dwight,DJ Thaad

### **SpeakerBio:**Yesterday & Tomorrow

No BIO available

### **SpeakerBio:**Terrestrial Access Network

No BIO available

### **SpeakerBio:**Hellacopta

No BIO available

### **SpeakerBio:**Hanz Dwight

No BIO available

### **SpeakerBio:**DJ Thaad

No BIO available

#### **Description:**

21:00 - 22:00: Terrestrial Access Network 22:00 - 23:00: DJ Thaad

23:00 - 00:00: Hellacopta

00:00 - 01:00: Hanz Dwight

01:00 - 02:00: Yesterday & Tomorrow

---

[Return to Index](#) - Add to [!\[\]\(a2c66188845a304b47cb41d1e0cbd777\_img.jpg\) Google Calendar](#) - ics [Calendar](#) file

---

## **SOC - Thursday - 21:00-01:59 PDT**

---

**Title:** Hallway Monitor Party - Entertainment

**When:** Thursday, Aug 11, 21:00 - 01:59 PDT

**Where:** Caesars Forum - Skybridge Entrance

**Speakers:**Tavoo,PankleDank,Heckseven,DotOrNot,CodexMafia

**SpeakerBio:**Tavoo

No BIO available

**SpeakerBio:**PankleDank

No BIO available

**SpeakerBio:**Heckseven

No BIO available

**SpeakerBio:**DotOrNot

No BIO available

**SpeakerBio:**CodexMafia

No BIO available

#### **Description:**

21:00 - 22:00: heckseven

22:00 - 23:00: DotOrNot

23:00 - 00:00: Tavoo

00:00 - 01:00: CodexMafia

01:00 - 02:00: PankleDank

[Return to Index](#) - Add to



- ics [Calendar](#) file

## **HRV - Saturday - 11:30-11:59 PDT**

**Title:** Ham Nets 101

**When:** Saturday, Aug 13, 11:30 - 11:59 PDT

**Where:** Flamingo - Virginia City II

**SpeakerBio:**Jon Marler

Jon is a product manager at Viking Cloud with a true passion for information security. Jon is an amateur radio operator, lockpicker, phreaker, repairer of all things, and maker.

Twitter: [@https://twitter.com/jmarler](https://twitter.com/jmarler)

#### **Description:**

Ham Nets 101 - An introduction to ham nets for operators of all experience levels. Nets are an easy way to get on the air, talk to other hams, and be part of the ham community. Ham nets operate on all bands and often even on local repeaters. If you have a brand new Technician license, or a dusty old Extra, come learn all about what ham nets are and how to participate.

[Return to Index](#) - Add to



- ics [Calendar](#) file

**Title:** Hand On Mainframe Buffer Overflows - RCE Edition

**When:** Friday, Aug 12, 15:00 - 18:59 PDT

**Where:** Harrah's - Elko

**Speakers:** Phil Young, Jake Labelle

**SpeakerBio:** Phil Young , Mainframe Security Expert

Philip Young, aka Soldier of FORTRAN, is a leading expert in all things mainframe hacking. Having spoken and taught at conferences around the world, including DEFCON, RSA, BlackHat and keynoting at both SHARE and GSE Europe, he has established himself as the thought leader in mainframe penetration testing. Since 2013 Philip has released tools to aid in the testing of mainframe security and contributed to multiple open source projects including Nmap, allowing those with little mainframe capabilities the chance to test their mainframes. His hope is that through raising awareness about mainframe security more organizations will take their risk profile seriously.

**SpeakerBio:** Jake Labelle , Security Consultant

Jake, a security consultant from Basingstoke, UK, got his hands on a licensed emulator for z/OS over the pandemic , and considering that we have been in and out of lockdown for the past two years, started playing around with it for a fairly good portion of time. As someone who adores the 80s cyber aesthetic, he loves mucking around with it, but also there is nothing legacy about mainframes, docker, node js, python all your modern applications/programs are on there. Over the past year, he has found and reported a number of z/OS LPEs and RCEs vulns to IBM.

Twitter: [@https://twitter.com/Jabellz2](https://twitter.com/Jabellz2)

**Description:**

For decades mainframes have been thought to be unhackable. One of the core tenants of this myth was that buffer overflows were not possible on MVS. In 2020 a mainframe hacker figured out how to find and exploit z/OS binaries using very simple buffer overflow techniques. This workshop aims to teach you those techniques. Attendees will learn how C programs are used on mainframes, understand how to use JCL for buffer overflows, how save areas are used, common registries used for pointers, ASCII to EBCDIC machine code, and how they can hunt vulnerable binaries in their environment. Multiple hands-on labs will be instructor lead with a real mainframe provided both during and after class.

**Materials**

A laptop capable of running a modern browser

**Prereq**

None

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## LPV - Friday - 15:30-15:45 PDT

---

**Title:** Handcuffs and how they work

**When:** Friday, Aug 12, 15:30 - 15:45 PDT

**Where:** Caesars Forum - Summit 203-204, 235

**SpeakerBio:** Steven Collins

No BIO available

**Description:**

High level explanation of how a handcuff actually works inside.

## IOTV - Sunday - 10:00-12:59 PDT

---

**Title:** Hands on hacking labs

**When:** Sunday, Aug 14, 10:00 - 12:59 PDT

**Where:** Caesars Forum - Alliance 311, 320

### Description:

IoT Hacking 101 is a set of quick, hands-on labs developed to teach the tools techniques for discovering and exploiting some of the common weaknesses found in IoT devices today. Whether you're a pentester that has never hacked IoT devices or even someone that has never hacked anything (!), these self-guided labs will walk you through all the steps in order to successfully pwn IoT.

---

## IOTV - Saturday - 10:00-17:59 PDT

---

**Title:** Hands on hacking labs

**When:** Saturday, Aug 13, 10:00 - 17:59 PDT

**Where:** Caesars Forum - Alliance 311, 320

### Description:

IoT Hacking 101 is a set of quick, hands-on labs developed to teach the tools techniques for discovering and exploiting some of the common weaknesses found in IoT devices today. Whether you're a pentester that has never hacked IoT devices or even someone that has never hacked anything (!), these self-guided labs will walk you through all the steps in order to successfully pwn IoT.

---

## IOTV - Friday - 10:00-17:59 PDT

---

**Title:** Hands on hacking labs

**When:** Friday, Aug 12, 10:00 - 17:59 PDT

**Where:** Caesars Forum - Alliance 311, 320

### Description:

IoT Hacking 101 is a set of quick, hands-on labs developed to teach the tools techniques for discovering and exploiting some of the common weaknesses found in IoT devices today. Whether you're a pentester that has never hacked IoT devices or even someone that has never hacked anything (!), these self-guided labs will walk you through all the steps in order to successfully pwn IoT.

---

## IOTV - Sunday - 10:00-12:59 PDT

---

**Title:** Hands on Hardware Hacking – eMMC to Root

**When:** Sunday, Aug 14, 10:00 - 12:59 PDT

**Where:** Caesars Forum - Alliance 311, 320

**SpeakerBio:**Deral Heiland

No BIO available

### Description:

Hardware hacking with Rapid7! Rapid7 guided exercises will lead you through the hands-on hardware hacking process to gain root level access to embedded IoT technology. This series of exercises will cover multiple steps including embedded multimedia controller (eMMC) interaction, making binary images copies of flash, interaction with read only squash files systems to unpack and repack systems, and altering startup files systems within the devices' file system to allow you to eventually gain root level access over SSH.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

## IOTV - Friday - 10:00-17:59 PDT

---

**Title:** Hands on Hardware Hacking – eMMC to Root

**When:** Friday, Aug 12, 10:00 - 17:59 PDT

**Where:** Caesars Forum - Alliance 311, 320

**SpeakerBio:**Deral Heiland

No BIO available

### Description:

Hardware hacking with Rapid7! Rapid7 guided exercises will lead you through the hands-on hardware hacking process to gain root level access to embedded IoT technology. This series of exercises will cover multiple steps including embedded multimedia controller (eMMC) interaction, making binary images copies of flash, interaction with read only squash files systems to unpack and repack systems, and altering startup files systems within the devices' file system to allow you to eventually gain root level access over SSH.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

## IOTV - Saturday - 10:00-17:59 PDT

---

**Title:** Hands on Hardware Hacking – eMMC to Root

**When:** Saturday, Aug 13, 10:00 - 17:59 PDT

**Where:** Caesars Forum - Alliance 311, 320

**SpeakerBio:**Deral Heiland

No BIO available

## Description:

Hardware hacking with Rapid7! Rapid7 guided exercises will lead you through the hands-on hardware hacking process to gain root level access to embedded IoT technology. This series of exercises will cover multiple steps including embedded multimedia controller (eMMC) interaction, making binary images copies of flash, interaction with read only squash files systems to unpack and repack systems, and altering startup files systems within the devices' file system to allow you to eventually gain root level access over SSH.

---

[Return to Index](#) - Add to



- ics [Calendar](#) file

---

## AIV - Saturday - 11:00-11:50 PDT

---

**Title:** Hands-on Hacking of Reinforcement Learning Systems

**When:** Saturday, Aug 13, 11:00 - 11:50 PDT

**Where:** Caesars Forum - Summit 228->236

**SpeakerBio:** Dr. Amanda Minnich

No BIO available

## Description:

Reinforcement learning (RL) is a class of machine learning where an agent learns the optimal actions to take to achieve short- and long-term objectives in the context of its environment. RL models are everywhere, from enabling autonomous vehicles to drive to assisting in diagnostic decision making in healthcare. They are used to make critical decisions with life-or-death implications, meaning the security and robustness of these models and the machine learning systems they comprise is extremely important.

However, the threat model of these RL systems is not well understood. Traditional network and system security measures are expected to provide some level of protection from threat actors, but if an attacker can get past these, many post-exploitation threat vectors exist in the reinforcement learning model itself, which can be weaponized and lead to disastrous outcomes.

In this talk, I will provide a high-level overview of reinforcement learning and the classes of attacks used to compromise RL systems. I will also present and demo two RL attacks we developed that do not require in-depth machine learning expertise to implement: the initial perturbation attack and the Corrupted Replay Attack (CRA), an attack we created while doing this research. Both of these attacks will be available as part of our open-source toolkit, Counterfit, so attendees can use these attacks against a reinforcement learning model of their choice. Finally, I will speak about my practical experiences in this space, describing the repercussions of an adversary successfully executing these attacks in the wild.

Attendees will walk away from this talk with the knowledge and tools to attack RL models, as well as an appreciation for the importance of properly securing machine learning systems.

---

[Return to Index](#) - Add to



- ics [Calendar](#) file

---

## WS - Thursday - 10:00-13:59 PDT

---

**Title:** Hands-On TCP/IP Deep Dive with Wireshark - How this stuff really works

**When:** Thursday, Aug 11, 10:00 - 13:59 PDT

**Where:** Harrah's - Reno

## **SpeakerBio:**Chris Greer , Network Analyst & Wireshark Instructor

Chris Greer is a Packet Head. He is a Packet Analyst and Trainer for Packet Pioneer, a Wireshark University partner, and has a passion for digging into the packet-weeds and finding answers to network and cybersecurity problems. Chris has a YouTube channel where he focuses on videos showing how to use Wireshark to examine TCP connections, options, and unusual behaviors, as well as spotting scans, analyzing malware, and other IOC's in the traffic. His approach to training is that if you aren't having fun doing something, you won't retain what you are learning, so he strives to bring as much hands-on and humor to the classroom as possible. Chris remembers what it was like to look at Wireshark for the first time, and knows how complicated packet analysis can be. With that in mind, he has designed an easy-to-follow course that will appeal both to the beginner and more advanced Packet Person.

Twitter: [@https://twitter.com/packetpioneer](https://twitter.com/packetpioneer)

## **Description:**

Let's break out Wireshark and dig deep in to the TCP and IP protocols. This skill is critical for anyone interested in any area of cybersecurity, no matter the color of the hat. Almost all enumeration, scans, incident response, and traffic forensics require the analyst to dig into and interpret TCP conversations. When enumerating an environment, identifying key TCP/IP indicators in protocol headers can also help when passively fingerprinting systems.

In this workshop we will roll back our sleeves and learn how TCP/IP really works - the handshake, options, sequence/ack numbers, retransmissions, TTL, and much more. This workshop welcomes all cybersecurity and wireshark experience levels.

### Materials

Just a laptop with a copy of Wireshark. I will provide the sample pcaps for analysis.

### Prereq

None

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## **BTW - Friday - 15:00-15:59 PDT**

---

**Title:** Heavyweights: Threat Hunting at Scale

**When:** Friday, Aug 12, 15:00 - 15:59 PDT

**Where:** Flamingo - Savoy Ballroom - BTV Main Stage

**Speakers:**Sherrod DeGrippo,Ashlee Benge,Jamie Williams,nohackme,Sean Zadig,Ryan Kovar

### **SpeakerBio:**Sherrod DeGrippo

Sherrod DeGrippo is the Vice President of Threat Research and Detection for Proofpoint, Inc. She leads a worldwide malware research team to advance Proofpoint threat intelligence and keep organizations safe from cyberattacks. With more than 17 years of information security experience.

### **SpeakerBio:**Ashlee Benge

No BIO available

### **SpeakerBio:**Jamie Williams

Jamie is an adversary emulation engineer for The MITRE Corporation where he works with amazing people on various exciting efforts involving security operations and research, mostly focused on adversary emulation and behavior-based detections. He leads the development of MITRE ATT&CK® for Enterprise and has also led teams that help shape and deliver the “adversary-touch” within MITRE Engenuity ATT&CK Evaluations as well as the Center for Threat-Informed Defense (CTID).

### **SpeakerBio:**nohackme

Mick Baccio fell in love with the idea of cybersecurity at nine years old after reading Neuromancer, thinking "I should do that." After an alphabet soup of federal agencies and a stint as the first CISO of a POTUS campaign, he is currently a Global Security Advisor at Splunk SURGe. He is still trying to do 'that'. Air Jordans, Thrunting, Puns. Not sure the order.

### **SpeakerBio:**Sean Zadig

No BIO available

### **SpeakerBio:**Ryan Kovar

No BIO available

### **Description:**

Panel Discussion discussing how evolving techniques for defenders is amplified, from some of the teams behind the blogs.

Panel Discussion discussing how evolving techniques for defenders is amplified, from some of the teams behind the blogs.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## **MIV - Friday - 16:00-16:59 PDT**

---

**Title:** History of Russian Cyber & Information Warfare (2007-Present)

**When:** Friday, Aug 12, 16:00 - 16:59 PDT

**Where:** Caesars Forum - Summit 221->236

### **SpeakerBio:**Ryan Westman

As Senior Manager of Threat Intelligence, Ryan is responsible for demystifying the Threat Landscape for eSentire's Threat Response Unit. His goal is to detect and respond to threats before they become risks to eSentire's client base. Prior to eSentire, Ryan spent three years at Deloitte helping build, develop, and establish a Threat Intelligence & Analytics team. Ryan holds a BA in Political Science & History from Wilfrid Laurier University, a MSc in Counter-Terrorism from the University of Central Lancashire where he conducted primary research on individuals perceptions of terrorism through Social Media, and a Master's degree from the University of Waterloo. He is a GIAC Certified Cyber Threat Intelligence Analyst.

**Description:**No Description available

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## **MIV - Friday - 16:00-16:59 PDT**

---

**Title:** History of the weaponization of social media

**When:** Friday, Aug 12, 16:00 - 16:59 PDT

**Where:** Caesars Forum - Summit 221->236

### **SpeakerBio:**Gina Rosenthal , Independent

Gina Rosenthal has worked for the big infrastructure companies for many years. She helped start social media programs in those companies, and has always fought for people over stats. She also was an activist in college, helping found the American Indian Student Union at a big football school that has a native mascot. When she started her company, part of what she intended to do was help people understand what it means to have digital literacy.

**Description:**No Description available

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

## DL - Saturday - 14:00-15:55 PDT

**Title:** hls4ml - Open Source Machine Learning Accelerators on FPGAs

**When:** Saturday, Aug 13, 14:00 - 15:55 PDT

**Where:** Caesars Forum - Council Boardroom

**Speakers:**Ben Hawks,Andres Meza

### **SpeakerBio:**Ben Hawks

Ben Hawks is an AI Researcher at Fermi National Accelerator Laboratory, focusing on optimizing and compressing neural networks to be tiny, fast, and accurate for use on FPGAs and other specialized hardware. Since he was young, he's had a personal interest in computer security, programming, and electronics, and is interested in learning how to make machine learning fair, efficient, and fast. Outside of work, he spends his time messing with electronics, tabletop RPGs, and catering to the whims of a small feline overlord.

### **SpeakerBio:**Andres Meza

Andres Meza is a research and development engineer in the Department of Computer Science and Engineering at the University of California, San Diego. He received a B.S. Computer Science and a B.S. Cognitive Science with a Machine Learning and Neural Computation Specialization from UCSD in 2020. His current research focuses on hardware security, optimization of ML models for hardware deployment, and computer vision.

### **Description:**

Born from the high energy physics community at the Large Hadron Collider, hls4ml is an open-source Python package for machine learning inference in FPGAs (Field Programmable Gate Arrays). It creates firmware implementations of machine learning algorithms by translating traditional, open-source machine learning package models into optimized high level synthesis C++ that can then be customized for your use case and implemented on devices such as FPGAs and Application Specific Integrated Circuits (ASICs). Hls4ml can easily scale the implementation of a model to take advantage of the parallel processing capabilities that FPGAs offer, not only allowing for low latency, high throughput designs, but also designs sized to fit on lower cost, resource constrained hardware. Hls4ml also supports generating accelerators with different drivers that build minimal, self-contained implementations which enable control via Python or C/C++ with little extra development or hardware expertise.

Audience: Hardware, AI, IoT, FPGA

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

## BTW - Saturday - 15:00-15:15 PDT

**Title:** Horusec - Brazilian SAST help World

**When:** Saturday, Aug 13, 15:00 - 15:15 PDT

**Where:** Virtual - BlueTeam Village - Talks

### **SpeakerBio:**Gilmar Esteves

Gilmar works with information security2006. He was a Marine in the Brazilian Navy, worked in large telecom and payments

companies. He is currently Vice President of Information Security and coordinates some research fronts in addition to the day to day of Cyber.

## Description:

Demonstrate how Horusec can help and how easy it is to get started. Show the evolutions of the latest version and invite people to contribute. Show the case of Log4j where we became Top Trend on Twitter because of the detection and after that several big companies started using it.

Demonstrate from installation to configuration to detection and how AppSec and BlueTeam times can benefit.

Presentation of the Horusec tool (<https://github.com/ZupIT/horusec>) that was developed by ZUP IT in Brazil to help companies identify security problems in the most common languages still in a development environment or the IDE.

---

[Return to Index](#) - Add to



- ics [Calendar](#) file

---

## WS - Thursday - 15:00-18:59 PDT

---

**Title:** House of Heap Exploitation

**When:** Thursday, Aug 11, 15:00 - 18:59 PDT

**Where:** Harrah's - Goldfield + Tonopah

**Speakers:**Nathan Kirkland,Maxwell Dulin,Kenzie Dolan,Zachary Minneker

### **SpeakerBio:**Nathan Kirkland

Raised on a steady diet of video game modding, when Nathan found programming as a teenager, he fit right into it. Legend says he still keeps his coffee (and tear) stained 1980s edition of The C Programming Language by K&R stored in a box somewhere. A few borrowed Kevin Mitnick books later, he had a new interest, and began spending more and more time searching for buffer overflows and SQL injections. Many coffee fueled sleepless nights later, he had earned OSCP, and graduated highschool a few months later. After a few more years of working towards a math degree and trying fervently to teach himself cryptanalysis, he decided to head back to the types of fun hacking problems that were his real first love, and has worked at Security Innovation ever since.

### **SpeakerBio:**Maxwell Dulin , Security Engineer

Maxwell Dulin (Strikeout) is a senior security consultant hacking all things under the sun, from garage doors to web applications to operating systems. Maxwell has published many articles/talks for a plethora of heap exploitation techniques, assorted web application exploits and IoT devices. He has previously spoken at DEF CON 27s IoT Village, ToorCon, CanSecWest, Hackfest and DEF CON workshops. His research is focused on custom RF protocols and binary exploitation methods. In his free time, he plays with RF toys, hikes to fire lookouts and catches everything at dodgeball.

Twitter: [@https://twitter.com/Dooflin5](https://twitter.com/Dooflin5)

### **SpeakerBio:**Kenzie Dolan , Security Engineer

Kenzie Dolan (they/she) works for Security Innovation as a Security Engineer focusing on engagements ranging from IoT hacking to kiosk exploitation. His current research interests include emerging threats against Mobile and IoT devices. He has a degree in Computer and Information Science from University of Oregon. In his free time, James enjoys composing music, playing video games or hiking in the greater Seattle area.

### **SpeakerBio:**Zachary Minneker , Senior Security Engineer, Security Innovation

Zachary Minneker is a senior security engineer and security researcher at Security Innovation. His first computer was a PowerPC Macintosh, an ISA which he continues to defend to this day. At Security Innovation, he has performed security assessments on a variety of systems, including robots for kids, audio transcription codecs, and electronic medical systems. He has previous experience administrating electronic medical systems, and deep experience in fuzzing, reverse engineering, and

protocol analysis. His research has focused on techniques for in-memory fuzzing, IPC methods, and vulnerability discovery in electronic medical record systems and health care protocols. In his free time he works on music and synthesizers.

Twitter: [@https://twitter.com/seiranib](https://twitter.com/seiranib)

## Description:

### Materials

Laptop with enough power for a moderately sized Linux VM Administrative access to the laptop 8GB RAM minimum 30GB harddrive space Virtualbox or another virtualization platform installed

### Prereq

Basic computer science background (x86\_64 assembly, stack, programming skills in C & Python) Basic binary exploitation skills (buffer overflow exploitation, ROP, ASLR, etc.) - Familiar with Linux developer tools such as the command line, Python scripting and GDB.

[Return to Index](#) - Add to



- ics [Calendar](#) file

## DDV - Friday - 13:00-13:59 PDT

**Title:** How long do hard drives and SSDs live, and what can they tell us along the way?

**When:** Friday, Aug 12, 13:00 - 13:59 PDT

**Where:** Flamingo - Exec Conf Ctr - Lake Meade and Valley of Fire

### SpeakerBio: Andrew Klein

Andy has 25 years experience in the cloud storage, email security, and network security fields. Prior to Backblaze he worked at Symantec, Checkpoint, PGP, and PeopleSoft, as well as startups throughout Silicon Valley. He has presented at the Federal Trade Commission, DEFCON 26 (DDV), RSA, MSST, SNIA/SDC, InfoSecurity, InterOp, and other security and cloud storage events in the US and Europe.

## Description:

Since 2013 Andrew's company has collected daily operational data from the hard drives and SSDs in our data centers. This includes daily SMART statistics from over 250,000 drives totaling over 2 Exabytes of storage. We've reviewed and analyzed this data and we would like to share what we've learned including the most current annualized failure rates for the hard drive and SSDs we use which we'll present model-by-model and by manufacture and size. We'll show, explain, and compare the life expectancy curves for several drive models we use including 4, 8, 12 and 14TB drives. We'll demonstrate how you can use SMART stats and Machine Learning techniques to predict drive failure, and we'll finish up by answering some drive mysteries like; is drive failure related to drive temperature, or using helium in the drive, or power-cycling the drive (turning it on and off on a regular basis)? As a bonus, we'll show you where to get the data so you can do your own analysis if you desire.

[Return to Index](#) - Add to



- ics [Calendar](#) file

## DC - Friday - 15:30-16:15 PDT

**Title:** How Russia is trying to block Tor

**When:** Friday, Aug 12, 15:30 - 16:15 PDT

**Where:** Caesars Forum - Forum 106-110, 138-139 (Track 2)

### SpeakerBio: Roger Dingledine , The Tor Project

Roger Dingledine is president and co-founder of the Tor Project, a nonprofit that develops free and open source software to protect people from tracking, censorship, and surveillance online.

Wearing one hat, Roger works with journalists and activists on many continents to help them understand and defend against the threats they face. Wearing another, he is a lead researcher in the online anonymity field, coordinating and mentoring academic researchers working on Tor-related topics. Since 2002 he has helped organize the yearly international Privacy Enhancing Technologies Symposium (PETS).

Among his achievements, Roger was chosen by the MIT Technology Review as one of its top 35 innovators under 35, he co-authored the Tor design paper that won the Usenix Security "Test of Time" award, and he has been recognized by Foreign Policy magazine as one of its top 100 global thinkers.

Twitter: [@https://twitter.com/RogerDingledine](https://twitter.com/RogerDingledine)

## Description:

In December 2021, some ISPs in Russia started blocking Tor's website, along with protocol-level (DPI) and network-level (IP address) blocking to try to make it harder for people in Russia to reach the Tor network. Some months later, we're now at a steady-state where they are trying to find new IP addresses to block and we're rotating IP addresses to keep up.

In this talk I'll walk through what steps the Russian censors have taken, and how we reverse engineered their attempts and changed our strategies and our software. Then we'll discuss where the arms race goes from here, what new techniques the anti-censorship world needs if we're going to stay ahead of future attacks, and what it means for the world that more and more countries are turning to network-level blocking as the solution to their political problems.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## BHV - Saturday - 16:30-17:59 PDT

---

**Title:** How to Build DIY Lifesaving Medical Devices

**When:** Saturday, Aug 13, 16:30 - 17:59 PDT

**Where:** Flamingo - Laughlin I,II,III

**SpeakerBio:**Four Thieves Vinegar Collective

No BIO available

Twitter: [@https://twitter.com/4ThievesVinegar](https://twitter.com/4ThievesVinegar)

## Description:

Over the course of the past two years, our group has finished a number of projects which allow for people to take control of their own health. Automatic external defibrillators can cause someone who is in [certain types of] cardiac arrest to merely wake up, but only if they get it soon enough. However, they cost thousands of dollars. We have an open-source version which can be built for \$500 by any mid-level hobbyist, and meets all CE and FDA requirements. Additionally, we have adjoint tools for the AED which increase the save rate, and reduce the likelihood of brain damage. We also have an open-source DIY automated chemical reactor, with which people can manufacture their own drugs. We will be demonstrating the device and releasing complete instructions and programs for it, including one which makes Narcan out of Vicodin. Lastly, we will have a live demonstration, and give public online access to an AI which can discover drug synthesis pathways. Come see all this and more, as we release detailed documentation explaining how to build devices yourself which can save your life.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

**Title:** How to do Cloud Security assessments like a pro in only #4Steps**When:** Sunday, Aug 14, 10:40 - 11:20 PDT**Where:** Flamingo - Scenic Ballroom**SpeakerBio:**Ricardo Sanchez

Ricardo Sanchez is a Senior cloud security expert with 10+ years of experience in security. He is currently leading the Cloud Security Unit in one of the larger focused cybersecurity firms in the Netherlands.

**Description:**

Cloud security is evolving rapidly and can be challenging. The growing need for remote working over the last year enhances this development. How can companies keep up with the pace of change? How do you know you are secure? Are the default installations secure? How do you find and fix your Cloud misconfigurations? How do you even start doing a Cloud assessment? Is it like an on-premise one? At the end of the conversation you will have a detailed guide with tools and examples of how can you hack/secure a cloud environment in only #4Steps.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

**DC - Saturday - 11:00-11:45 PDT****Title:** How To Get MUMPS Thirty Years Later (or, Hacking The Government via FOIA'd Code)**When:** Saturday, Aug 13, 11:00 - 11:45 PDT**Where:** Caesars Forum - Alliance 301-309, 321 (Track 4)**SpeakerBio:**Zachary Minneker , Senior Security Engineer, Security Innovation

Zachary Minneker is a senior security engineer and security researcher at Security Innovation. His first computer was a PowerPC Macintosh, an ISA which he continues to defend to this day. At Security Innovation, he has performed security assessments on a variety of systems, including robots for kids, audio transcription codecs, and electronic medical systems. He has previous experience administrating electronic medical systems, and deep experience in fuzzing, reverse engineering, and protocol analysis. His research has focused on techniques for in-memory fuzzing, IPC methods, and vulnerability discovery in electronic medical record systems and health care protocols. In his free time he works on music and synthesizers.

Twitter: [@https://twitter.com/seiranib](https://twitter.com/seiranib)**Description:**

In the 60s, engineers working in a lab at Massachusetts General Hospital in Boston invented a programming environment for use in medical contexts. This is before C, before the Unix epoch, before the concept of an electronic medical records system even existed. But if you have medical records in the US, or if you've banked in the US, its likely that this language has touched your data. Since the 1960s, this language has been used in everything from EMRs to core banking to general database needs, and even is contained in apt to this day.

This is the Massachusetts General Hospital Utility Multi-Programming System. This is MUMPS.

This talk covers new research into common open-source MUMPS implementations, starting with an application that relies on MUMPS: the Department of Veterans Affairs' VistA EMR. We'll cover a short history of VistA before diving into its guts and examining MUMPS, the language that VistA was written in. Then we'll talk about 30 memory bugs discovered while fuzzing open source MUMPS implementations before returning to VistA to cover critical vulnerabilities found in credential handling and login mechanisms. We'll close by taking a step back and asking questions about how we even got here in the first place, the right moves we made, and what we can do better.

## BHV - Saturday - 11:00-11:59 PDT

---

**Title:** How to Leverage MDS2 Data for Medical Device Security

**When:** Saturday, Aug 13, 11:00 - 11:59 PDT

**Where:** Flamingo - Laughlin I,II,III

**SpeakerBio:** Jeremy Linden

Jeremy Linden is Sr. Director, Product Management at Asimily. He has over 15 years of experience in the cybersecurity industry as a product manager, engineer, and security analyst. Prior to Asimily, he led product management teams at Expanse, OpenDNS, and other security companies.

Twitter: [@https://twitter.com/jeremydlinden](https://twitter.com/jeremydlinden)

**Description:**

The Manufacturers Disclosure Statement for Medical Device Security, or MDS2, has become increasingly ubiquitous as a source of information about the security capabilities of IoMT devices, but many organizations still find operationalizing the information contained within to be challenging. In this talk, learn how to best analyze the MDS2 form to gather security data, and how to leverage the data contained within the MDS2 form to improve your IoMT security posture across the device lifecycle, both for pre-procurement risk assessments and post-procurement management and hardening.

---

## CPV - Friday - 13:30-13:59 PDT

---

**Title:** How to Respond to Data Subject Access Requests

**When:** Friday, Aug 12, 13:30 - 13:59 PDT

**Where:** Flamingo - Vista Ballroom

**SpeakerBio:** Irene Mo

Irene Mo is an associate with Hintze Law PLLC, a boutique privacy firm providing counseling exclusively on global data protection.

Irene counsels clients on a wide range of privacy and data security issues, including conducting and setting up Records of Processing Activities, Data Protection Impact Assessments, implementing global data protection programs, and integrating privacy protections into emerging technology. Irene has experience with the California Consumer Protection Act, EGeneral Data Protection Regulation, the Federal Trade Commission Act, Health Insurance Portability and Accountability Act Privacy Rule, and cybersecurity.

Before Hintze Law, Irene was a Senior Associate at Aleada Consulting and gained valuable experience as a legal technology consultant helping organizations with project management, lean-process improvement, content creation, and community building.

As Community Lead for Women in Security and Privacy, Irene helps with fundraising and event planning by fostering engagement with WISP's corporate sponsors.

**Description:**

International and United States privacy laws provide individuals with rights to the personal information companies have about them. One of the most exercised rights is the right to access personal information. This talk will explain: 1) what are data subject rights; 2) who has these rights; 3) how to respond to access requests; 4) methods for responding to data subject rights requests; and 5) what to know before implementing a privacy automation vendor.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## BHV - Friday - 12:30-13:30 PDT

---

**Title:** How to stop Surveillance Capitalism in Healthcare

**When:** Friday, Aug 12, 12:30 - 13:30 PDT

**Where:** Flamingo - Laughlin I,II,III

**Speakers:**Andrea Downing,Jillian Simons,Valencia Robinson

### **SpeakerBio:**Andrea Downing

Andrea Downing is a cancer advocate turned security researcher. Her work has been featured on CNN, Fortune, and The Verge, and has catalyzed an urgent dialogue on national health privacy policy and the need for protections outside of HIPAA. Andrea has co-founded a nonprofit called The Light Collective to work with vulnerable patient groups seeking digital rights and safe spaces for patient support communities on social media.

### **SpeakerBio:**Jillian Simons

Jillian Simons is a passionate advocate for the rights of individuals when it comes to data privacy and protection. She is a U.S. Navy veteran with 18 years of experience in data privacy and security, served eight years in the military as a cybersecurity analyst. Her work focuses on consumer rights and corporate obligations relating to data privacy and security. Jillian also has intellectual property experience in the health/life sciences industry and is a graduate of Harvard Law School, where she focused on policy and cyberlaw, and Georgetown University, where she focused on leadership and ethics.

### **SpeakerBio:**Valencia Robinson

Valencia Robinson is a breast cancer survivor, co-founding member of The Light Collective. As a patient advocate with 15 years experience working in the breast cancer community, Valencia is working to advance digital rights for patients and ensure technologies affecting the lives of her community have representation from people of color in the governance and design.

### **Description:**

The Light Collective will share how ad targeting tools in healthcare leak PHI from hospitals and other HIPAA covered entities at an unprecedented scale. We'll cover the ways surveillance capitalism in healthcare has caused harm to patient populations during the pandemic. We'll walk through common marketing tactics and techniques used in healthcare which create an effective kill chain when exploited. Finally, we'll discuss legal & policy implications.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## SKY - Friday - 10:35-11:25 PDT

---

**Title:** Hundreds of incidents, what can we share?

**When:** Friday, Aug 12, 10:35 - 11:25 PDT

**Where:** LINQ - BLOQ

**Speakers:**Brenton Morris,Guy Barnhart-Magen

## **SpeakerBio:**Brenton Morris

Sr Incident Responder at Profero. Brenton leads Incident Response engagements on a daily basis. From sophisticated cloud attackers to ransomware events. Brenton has a unique set of combined security research and developer experience, allowing him to resolve many cyber-attacks while fully understanding the impact on production systems.

Twitter: [@https://twitter.com/\\_scrapbird](https://twitter.com/_scrapbird)

## **SpeakerBio:**Guy Barnhart-Magen

With nearly 25 years of experience in the cyber-security industry, Guy held various positions in both corporates and startups.

In his role as the CTO for the Cyber crisis management firm Profero his focus is making incident response fast and scalable, harnessing the latest technologies and a cloud native approach.

Most recently, he led Intel's Predictive Threat Analysis group who focused on the security of machine learning systems and trusted execution environments. At Intel, he defined the global AI security strategy and roadmap. He spoke at dozens of events on the research he and the group have done on Security for AI systems and published several whitepapers on the subject.

Guy is the BSidesTLV chairman and CTF lead, a Public speaker in well known global security events (SAS, t2, 44CON, BSidesLV, and several DefCon villages to name a few), and the recipient of the Cisco "black belt" security ninja honor – Cisco's highest cybersecurity advocate rank.

He started as a software developer for several security startups and later spent eight years in the IDF. After completing his degrees in Electrical Engineering and Applied Mathematics, he focused on security research, in real-world applications.

He joined NDS (later acquired by Cisco). He led the Anti-Hacking, Cryptography, and Supply Chain Security Groups (~25 people in USA and Israel).

Twitter: [@https://twitter.com/barnhartguy](https://twitter.com/barnhartguy)

## **Description:**

There are two types of organizations, those that were breached and those that are not yet...

For most organizations, it is easier to buy blinky lightboxes and tick various compliance boxes (ISO27001 looking at you!) than improve their security posture.

We repeatedly see in the field that the vast majority of incidents could have been contained or even prevented if the effort had been spent in the right place.

We have some good statistics on what works, what can help, and what is generally a waste of effort with hundreds of incidents handled.

Most of the organizations that we see get breached are not Fortune 500 companies; they don't have colossal security budgets - but they do have a dedicated team that is doing their best to make a difference.

In this talk, we will cover some of our experience in what works in the real world and how you can focus your efforts on getting the correct data to respond and close incidents fast.

Invariably, the goal is not to have 100% security (no one will fund that!) but to get the business back on its feet ASAP and resume business operations. Planning for that takes dedication and focus - but it can be done!

we will focus in our talk on the pillars that would make your incident response plan work: Getting the right team in place  
Communication!

Data collection, access to systems

Access to forensics and response tools when you need them

This talk will outline common gaps and compare examples of these two types of organizations from actual incidents to highlight the real-life implications of lack of preparation, which affects the outcome of an incident.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## DC - Friday - 17:00-17:45 PDT

---

**Title:** Hunting Bugs in The Tropics

**When:** Friday, Aug 12, 17:00 - 17:45 PDT

**Where:** Caesars Forum - Forum 104-105, 135-136 (Track 1)

**SpeakerBio:** Daniel Jensen

Daniel (aka dozer) works as a security consultant at a large cybersecurity company. He has been a professional penetration tester for several years, and has discovered numerous vulnerabilities in a wide range of software. He currently lives in New Zealand, and his favourite animal is the goose.

Twitter: [@https://twitter.com/dozernz](https://twitter.com/dozernz)

### Description:

Aruba Networks makes networking products for the enterprise. I make enterprise products run arbitrary code.

Over the past couple of years, I've been hunting for vulnerabilities in some of Aruba's on-premise networking products and have had a bountiful harvest. A curated (read: patched) selection of these will be presented for your enjoyment. Pre-auth vulnerabilities and interesting bug chains abound, as well as a few unexpected attack surfaces and a frequently overlooked bug class.

This talk will explore some of the vulnerabilities I've found in various products in the Aruba range, and include details of their exploitation. I'll elaborate on how I found these bugs, detailing my workflow for breaking open virtual appliances and searching for vulnerabilities in them.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## ASV - Saturday - 13:00-13:50 PDT

---

**Title:** Hunting for Spacecraft Zero Days Using Digital Twins

**When:** Saturday, Aug 13, 13:00 - 13:50 PDT

**Where:** Caesars Forum - Forum 112-117

**SpeakerBio:** Brandon Bailey

Brandon Bailey is a pen-tester for gov and commercial sector and has worked in space cybersecurity for about 8years. He previously was a presenter at the Aerospace Village in 2020 and 2021. He has worked for NASA for over 10 years and was awarded NASA's Exceptional Service Medal for landmark cybersecurity work in 2019. Brandon currently work with Aerospace Corp.

### Description:

To ensure spacecraft architectures and software are built with security and resiliency, a focus on high-fidelity digital twins, purpose built for the testing need is recommended to perform research-based cyber evaluation and testing. This presentation will demonstrate how to use high fidelity digital twins for advanced cyber research. Focus will be applied on PowerPC750 environment.

## BTV - Saturday - 14:15-14:45 PDT

**Title:** Hunting Malicious Office Macros

**When:** Saturday, Aug 13, 14:15 - 14:45 PDT

**Where:** Virtual - BlueTeam Village - Talks

**SpeakerBio:** Anton Ovrutsky

Anton is a BSides Toronto speaker, C3X volunteer, and an OSCE, OSCP, CISSP, CSSP certificate holder. Anton enjoys the defensive aspects of cybersecurity and loves logs and queries.

### Description:

The talk will cover the following areas:

- Baselining Office macros behaviors
- Contextualized / Risk-based alerting strategies
- Data sets & Sysmon configurations will be provided
- Coverage of new attack vectors such as mark of the web bypasses and VSTO files

When reviewing threat intelligence reports it is common to see malicious Office macros of various types used as an initial access vector. Recently, Microsoft announced big changes to Office behavior in the context of malicious macros. However, organizations still struggle with detecting malicious macros which is often a prerequisite for implementing any type of hardening changes. The aim of this talk is to address this gap and provide guidance on how to detect malicious macro usage in environments and highlight the necessary steps to ensure systems are properly hardened against this threat.

## WS - Saturday - 15:00-18:59 PDT

**Title:** Hybrid Phishing Payloads: From Threat-actors to You

**When:** Saturday, Aug 13, 15:00 - 18:59 PDT

**Where:** Harrah's - Copper

**Speakers:** Magnus Stubman, Jon Christiansen

**SpeakerBio:** Magnus Stubman , Red Team

Magnus is part of the European Red Team at Mandiant and the APT66 project. He currently resides within the groups Malware team where he specializes in research and application of offensive techniques in both overt and covert engagements, discovering zero days and custom C2 techniques for the team. His other focuses is on adversarial simulation of FIN & APT groups via enactment of known (and not so known) TTPs, incorporating the known bad into something that can be used as a force of good.

**SpeakerBio:** Jon Christiansen , Red Team Lead

Jon is the Red Team lead for Mandiant Europe. After spending a decade as a hands-on keyboard Red Teamer and malware dev, he recently took a step back to focus more on capability development and team expansion. He founded the APT66 research project team at Mandiant and currently focuses research interest in the latest bypass techniques, threat actor malware and in finding new ways to jump the IT/OT barrier.

## Description:

The hard outer shell of cyber defenses often give way to a soft, gooey and easy-to-exploit centre, but all the lateral movement and escalation techniques in the world, isn't going to be worth anything if initial access cannot be secured. For threat actors and Red Teamer's alike, getting over that initial hurdle can be a long, arduous task with little hope of success and phishing in particular is often the bane of any aspiring attacker. Between EDRs, email scanner solutions, payload fingerprinting... what do you do?

This workshop has been developed with the aim of giving participants hands-on experience working with sophisticated payloads and techniques used by nation-state threat actors. Armed with payload automation tools, participants will learn to implement novel bypass techniques to circumvent state of the art anti-malware security products, both network-based and host-based technical controls, and iteratively improve their payloads throughout.

Topics will include:

- \* Multiple payload formats, the advantages and disadvantages
- \* Combining phishing techniques
- \* Automation, obfuscation and creation of payloads for quick turn around
- \* How to Improve payloads based on information gathered from earlier attacks
- \* Extracting technical information from threat actor intelligence breakdowns

## Materials

Just the laptop

## Prereq

Laptop with ability to connect to local network and run 1 VM requiring 4GB of memory Some understanding of phishing and what a payload is also a good idea Experience with creating / modifying tools from source code will also help

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## AIV - Friday - 11:00-11:50 PDT

---

**Title:** I'm not Keylogging you! Just some benign data collection for User Behavior Modeling

**When:** Friday, Aug 12, 11:00 - 11:50 PDT

**Where:** Caesars Forum - Summit 228->236

**SpeakerBio:** Harini Kannan

No BIO available

## Description:

User and Entity Behavior Analysis (UEBA) has been an active area of research in cybersecurity for years now. Advancements in unsupervised machine learning methodologies have made UEBA models effective in detecting anomalous drifts from baseline behavior. But when collecting user generated systems data from a cluster of machines in the cloud or from an endpoint, the data scientist gets access to human generated raw features, which keys are typed when, and what are those. This starts off as acceptable but wades into the grey area of almost keylogging users which is dangerous.

In this talk, we will go through a real example of how a user behavior experiment was set up, right from building the features to running the data collection script within containers to flushing the raw data regularly and the users sending only aggregated metrics to the data scientists for model building and analysis. We'll go through the entire setup from data collection and data flushing to model building by creating weak labels and further analysis.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

**Title:** ID theft insurance - The Emperor's new clothes?

**When:** Friday, Aug 12, 15:00 - 15:30 PDT

**Where:** Flamingo - Vista Ballroom

**SpeakerBio:** Per Thorsheim

Per Thorsheim is the founder of PasswordsCon, a conference dedicated to passwords, pins & anything digital authentication. By night he tries to fix security & privacy issues on the Internet, especially concerning DNS, email & authentication. He revealed LinkedIn got breached in 2012, and got personally involved with the Ashley Madison breach in 2015, both topics of previous talks in Vegas, including at CPV. He is well known for his presentation skills, and if you read all the way to here: he claims to know your next password.

**Description:**

You've got ID theft insurance bundled with other insurance products. No, you can't unselect the id theft insurance part. No, you can't have just one of them, & you pay for all of them. They are not valid if you get fooled/tricked. The insurance is not valid if the theft is committed by close relatives. The insurance is not valid if they don't target you personally, outside of work. They will not cover any monetary losses you may suffer, but will pay lawyers to tell you how to try to clean up your digital life - no guarantees provided. The primary business of the id theft insurance company is building effective customer loyalty programs through data collection & management. Oh, and they will use your personal data to «search for your personal data on the dark web to see if it has already leaked».

What could possibly go wrong?

This is my story, after I fell into a rabbit hole of security & privacy issues. Supposedly safe within the EU & GDPR borders governing my privacy.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

**PLV - Saturday - 10:00-11:45 PDT**

---

**Title:** Imagining a cyber policy crisis: Storytelling and Simulation for real-world risks

**When:** Saturday, Aug 13, 10:00 - 11:45 PDT

**Where:** Caesars Forum - Summit 226-227 - Policy Roundtable

**Speakers:** Winnona DeSombre, Safa Shahwan Edwards, Nina Kollars

**SpeakerBio:** Winnona DeSombre

No BIO available

**SpeakerBio:** Safa Shahwan Edwards , Deputy Director, Cyber Statecraft Initiative, Atlantic Council

No BIO available

**SpeakerBio:** Nina Kollars , Department of Defense

No BIO available

**Description:**

Story time for hackers. The importance of storytelling and simulation for teaching and training policymakers including a scenario from the Atlantic Council Cyber 9/12 program and other comparable efforts. Hear from panelists on how they construct stories and simulations for policymakers, from short from prose to war games to student competitions. This panel

draws on the hacking community's rich history of storytelling through fiction, graphic art, and more to demonstrate the practical importance of shaping ideas in policy debates. This session complements an otherwise heavy emphasis throughout the track on ideas over the medium itself. Panelists would also discuss their approach to breaking down a complicated issue or problem in order to represent its core themes, challenges, and opportunities especially for policymakers.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## PLV - Sunday - 10:00-11:45 PDT

---

**Title:** Improving International Vulnerability Disclosure: Why the US and Allies Have to Get Serious

**When:** Sunday, Aug 14, 10:00 - 11:45 PDT

**Where:** Caesars Forum - Summit 224-225 - Policy Collaboratorium

**Speakers:**Stewart Scott,Christopher Robinson

**SpeakerBio:**Stewart Scott , Assistant Director

Stewart Scott is an assistant director with the Cyber Statecraft Initiative under the Scowcroft Center for Strategy and Security at the Atlantic Council. His work there focuses on systems security policy, including software supply chain risk management, federal acquisitions processes, and open source software security. He holds a BA in Public Policy and a minor in Applications of Computing from Princeton University.

**SpeakerBio:**Christopher Robinson , Intel

No BIO available

### Description:

Join the Atlantic Council's Cyber Statecraft Initiative and DefCon Policy Track Initiative for a discussion on the strategic urgency behind better vulnerability disclosure. The session will focus on why the US and allied states need to take steps to make vulnerability disclosure easier, motivating the discussion with results from a study of the effects of a recently passed Chinese law on vulnerability disclosure.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## BTV - Friday - 13:00-13:59 PDT

---

**Title:** Improving security posture of MacOS and Linux with Azure AD

**When:** Friday, Aug 12, 13:00 - 13:59 PDT

**Where:** Virtual - BlueTeam Village - Talks

**Speakers:**Michael Epping,Mark Morowczynski

**SpeakerBio:**Michael Epping

Michael Epping is a Senior Product Manager in the Azure AD Engineering team at Microsoft. He is part of the customer experience team and his role is to accelerate the adoption of cloud services across enterprise customers. Michael helps customers deploy Azure AD features and capabilities via long-term engagements that can last years, as well as working within the engineering organization as an advocate on behalf of those customers. Michael has more than 9 years of experience working with customers to deploy Microsoft products like Azure AD, Intune, and Office 365.

**SpeakerBio:**Mark Morowczynski

Mark Morowczynski (@markmorow) is a Principal Program Manager on the customer success team in the Microsoft Identity

division. He spends most of his time working with customers on their deployments of Azure Active Directory. Previously he was PFE supporting Active Directory, Active Directory Federation Services and Windows Client performance. He was also one of the founders of the AskPFEPlat blog. He's spoken at various industry events such as Black Hat, Defcon Blue Team Village, Blue Team Con, GrayHat, several BSides, Microsoft Ignite, Microsoft MVP Summits, The Experts Conference (TEC), The Cloud Identity Summit, SANs Security Summits and TechMentor.

## Description:

We are from the Microsoft identity product group responsible for Active Directory and Azure Active Directory. We've noticed many customers struggle to deliver a good end user experience to their Apple and Linux Platforms. There are various ways to do this, but many customers are simply unaware of recommended configurations and best practices. This will be a deeply technical session that focuses not only on what can be done to improve this experience, but how the underlying Microsoft, Linux, and Apple technologies can work better together.

Most organizations have Windows, MacOS and Linux in their environment. Typically many of the security controls that are applied to Windows are not applied to MacOS or Linux, due to the size of the footprint and the difficulty of implementation. This can lead to holes in an organization's overall security posture as well as a poor end user experience.

Recently, Azure AD has released some new functionality to help improve the overall environment security posture for MacOS and Linux, both servers and clients. We'll discuss how these pieces work deep down and some best practices on deploying them.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## MIV - Friday - 16:00-16:59 PDT

---

**Title:** Information Confrontation 2022 - A loud war and a quiet enemy

**When:** Friday, Aug 12, 16:00 - 16:59 PDT

**Where:** Caesars Forum - Summit 221->236

**SpeakerBio:**Luke Richards

Luke Richards has many years of experience in IT and cyber security, having built corporate networks and complex applications, through to running threat intelligence and incident response for organizations across the globe. Recently his focus has been trends in cyber security, information intelligence and how these relate to real world events.

**Description:**No Description available

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## HHV - Friday - 15:00-15:45 PDT

---

**Title:** Injectll-Hide: Build-Your-Own Hardware Implants

**When:** Friday, Aug 12, 15:00 - 15:45 PDT

**Where:** Flamingo - Exec Conf Ctr - Red Rock VI, VII, VII

**Speakers:**Jeremy Miller,Jonathan Fischer

**SpeakerBio:**Jeremy Miller

Jeremy Miller is a 12+ year security professional that has worked in various industries including life-sciences, finance, and retail. Jeremy has worked both sides of the security spectrum ranging from Security Research, Red Teaming and Penetration

Testing to Threat Intelligence and SOC Analyst. Jeremy currently works as a Security Technical Lead for an emerging R&D Life Science Platform where he works on product and infrastructure security.

### **SpeakerBio:**Jonathan Fischer

Jonathan Fischer is a hardware and IoT security enthusiast that started off designing, programming, and implementing electronic controls for industrial control systems and off-highway machinery. After a decade in that industry, Jonathan obtained his BS in Computer Science and transitioned over to the cyber security industry where he has been working as a Red Team consultant and researcher for more than five years at a Fortune 500. Since joining the cyber security industry, Jonathan has since earned various industry certifications (OSCP, GPEN, etc.) and continues to leverage his unique experience in his research into hardware hacking.

### **Description:**

Hardware implants are not a new topic; however, their evolution seems to have stagnated outside of closed source, for-profit solutions. The disadvantage to these is that they lack the customization to adapt to large targeted deployments. Open-source projects exist but focus more on individual workstations (dumb keyboards/terminals), relying on corporate networks for remote control. This leaves a gap that we decided to address with our research. Our solution is an open source, hardware implant which adopts IoT technologies, using non-standard channels to create a remotely managed mesh network of hardware implants. Attendees will learn how we created a new breed of open-source hardware implant, along with lessons that we learned throughout the project. Topics covered in this talk include a detailed dive into the hardware that we used, the evolution of the project from start to finish, the complete design of our project, and our lessons learned along the way. Attendees will also be able to interact with a live version of the project.

---

[Return to Index](#) - Add to



- ics [Calendar](#) file

---

### **DL - Saturday - 10:00-11:55 PDT**

---

**Title:** Injectyll-HIDE: Pushing the Future of Hardware Implants to the Next Level

**When:** Saturday, Aug 13, 10:00 - 11:55 PDT

**Where:** Caesars Forum - Council Boardroom

**Speakers:**Jonathan Fischer,Jeremy Miller

### **SpeakerBio:**Jonathan Fischer

Jonathan Fischer is a hardware and IoT security enthusiast that started off designing, programming, and implementing electronic controls for industrial control systems and off-highway machinery. After a decade in that industry, Jonathan obtained his BS in Computer Science and transitioned over to the cyber security industry where he has been working as a Red Team consultant and researcher for more than five years at a Fortune 500. Since joining the cyber security industry, Jonathan has since earned various industry certifications (OSCP, GPEN, etc.) and continues to leverage his unique experience in his research into hardware hacking.

### **SpeakerBio:**Jeremy Miller

Jeremy Miller is a 12+ year security professional that has worked in various industries including life-sciences, finance, and retail. Jeremy has worked both sides of the security spectrum ranging from Security Research, Red Teaming and Penetration Testing to Threat Intelligence and SOC Analyst. Jeremy currently works as a Security Technical Lead for an emerging R&D Life Science Platform where he works on product and infrastructure security.

### **Description:**

Enterprises today are shifting away from dedicated workstations, and moving to flexible workspaces with shared hardware peripherals. This creates the ideal landscape for hardware implant attacks; however, implants have not kept up with this shift. While closed source, for-profit solutions exist and have seen some recent advances in innovation, they lack the customization to adapt to large targeted deployments. Open-source projects exist but focus more on individual workstations (dumb

keyboards/terminals) relying on corporate networks for remote control. Our solution is an open source, hardware implant which adopts IoT technologies, using non-standard channels to create a remotely managed mesh network of hardware implants. Attendees will learn how to create a new breed of open-source hardware implants. Topics covered in this talk include the scaling of implants for enterprise takeover, creating and utilizing a custom C2 server, a reverse shell that survives screen lock, and more. They will also leave with a new platform from which to innovate custom implants. Live demos will be used to show these new tactics against real world infrastructure. This talk builds off of previous implant talks but will show how to leverage new techniques and technologies to push the innovation of hardware implants forward evolutionarily.

Audience: Offense and Red Teams with a focus on a hardware approach

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## DC - Saturday - 17:00-17:45 PDT

---

**Title:** Internal Server Error: Exploiting Inter-Process Communication with new desynchronization primitives

**When:** Saturday, Aug 13, 17:00 - 17:45 PDT

**Where:** Caesars Forum - Academy 401-410, 421 (Track 3)

**SpeakerBio:** Martin Doyhenard , Security Researcher at Onapsis

Martin is a security researcher at the Onapsis Research Labs. His work includes performing security assessment on SAP and Oracle products and detecting vulnerabilities in ERP systems. His research is focused on Web stack security, reverse engineering and binary analysis, and he is also an active CTF player.

Martin has spoken at different conferences including DEFCON, RSA, HITB and EkoParty, and presented multiple critical vulnerabilities.

Twitter: [@https://twitter.com/tincho\\_508](https://twitter.com/tincho_508)

### Description:

In this talk I will show how to reverse engineer a proprietary HTTP Server in order to leverage memory corruption vulnerabilities using high level HTTP protocol exploitation techniques. To do so, I will present two critical vulnerabilities, CVE-2022-22536 and CVE-2022-22532, which were found in SAP's proprietary HTTP Server, and could be used by a remote unauthenticated attacker to compromise any SAP installation in the world.

First, I will explain how to escalate an error in the request handling process to Desynchronize data buffers and hijack every user's account with Advanced Response Smuggling. Furthermore, as the primitives of this vulnerability do not rely on header parsing errors, I will show a new technique to persist the attack using the first Desync botnet in history. This attack will prove to be effective even in an "impossible to exploit" scenario: without a Proxy!

Next I will examine a Use-After-Free in the shared memory used for Inter-Process Communication. By exploiting the incorrect deallocation, I will show how to tamper messages belonging to other TCP connections and take control of all responses using Cache Poisoning and Response Splitting theory.

Finally, as the affected buffers could also contain IPC control data, I will explain how to corrupt memory address pointers and end up obtaining RCE.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

**Title:** International Government Action Against Ransomware

**When:** Saturday, Aug 13, 16:00 - 17:45 PDT

**Where:** Caesars Forum - Summit 224-225 - Policy Collaboratorium

**Speakers:** Adam Dobell, Irfan Hemani, Jen Ellis

**SpeakerBio:** Adam Dobell , First Secretary, Department of Home Affairs, Embassy of Australia

No BIO available

**SpeakerBio:** Irfan Hemani , Deputy Director - Cyber Security, Cyber Security and Digital Identity Directorate, UK

Department for Digital, Culture, Media and Sport

No BIO available

**SpeakerBio:** Jen Ellis , Vice President of Community and Public Affairs

No BIO available

### **Description:**

Ransomware attacks continue to abound and various governments around the world are very active on combatting this issue. This session would bring some of them together to discuss what's being done and where it needs to go. It's been a little over a year since the Colonial Pipeline, HSE, and JBS attacks put ransomware firmly on the agenda as a threat to national security and economic stability. Since then, we've seen ransomware attacks become more openly politicized. We've also seen the White House and G7 both host international government forums to identify collaborative actions to tackle the threat. We've also seen new sanctions, public/private initiatives, bounties for criminals, and various other government actions introduced to make life for cybercriminals harder. This session brings together multiple govts to talk about what's being done, what results have been seen, and where we're headed next. They will start off covering these points and then open to the audience for questions and open discussion on next steps and impacts.

---

[Return to Index](#) - Add to



- ics [Calendar file](#)

---

## **SKY - Saturday - 13:50-15:40 PDT**

---

**Title:** INTERNET WARS 2022: These wars aren't just virtual

**When:** Saturday, Aug 13, 13:50 - 15:40 PDT

**Where:** LINQ - BLOQ

**Speakers:** Jivesx, Russ Handorf, Chris Kubecka, Harri Hursti, Cheryl Biswall, Bryson Bort, Gadi Evron

**SpeakerBio:** Jivesx

Jivesx is a 20 year veteran of network security, forensics and privacy in open higher ed environments. In his free time he tries to support the infosec community by volunteering, organizing, or just being a pest at multiple cons and villages.

Twitter: [@https://twitter.com/jivesx](https://twitter.com/jivesx)

**SpeakerBio:** Russ Handorf

Dr. Russell Handorf currently is an agent of chaos at Twitter. He is also recovering fed after ten years of service defending the USA and other countries in a variety of matters. He's done a lot of other odd things here and there, but that isn't important. Let's just have a conversation, but you'll have to endure my dad jokes.

Twitter: [@https://twitter.com/dntlookbehindu](https://twitter.com/dntlookbehindu)

## **SpeakerBio:**Chris Kubecka

CEO of cyber warfare incident management company in The Netherlands and Distinguished Chair for a Cyber Security program in the US Program. Advises the multiple governments, militaries, television and documentary technical advisor as a subject matter expert on cyber warfare national defense. Author of OSINT books and USAF military combat veteran, former military aircrew, and USAF Space Command. Defends critical infrastructure and handles country level cyber incidents, cyberwarfare, and cyber espionage. Lives and breathes IT/IOT/ICS SCADA control systems security. Hacker since the age of 10 and was in Kiev when the war started.

Twitter: [@https://twitter.com/SecEvangelism](https://twitter.com/SecEvangelism)

## **SpeakerBio:**Harri Hursti

Harri Hursti is a founder of Nordic Innovation Labs and the Voter Village. His work has been featured in two HBO documentaries, the latest being "Kill Chain: The Cyber War on America's Elections."

Twitter: [@https://twitter.com/HarriHursti](https://twitter.com/HarriHursti)

## **SpeakerBio:**Cheryl Biswall

Cheryl Biswas is a strategic Cyber Threat Intelligence Specialist at a major bank, a founder of The Diana Initiative and was featured in "Tribe of Hackers: Cybersecurity Advice from the Best Hackers in the World."

Twitter: [@https://twitter.com/3ncr1pt3d](https://twitter.com/3ncr1pt3d)

## **SpeakerBio:**Bryson Bort

Bryson is the Founder of SCYTHE and GRIMM, and Co-Founder of the ICS Village, a 501c3. 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.

Twitter: [@https://twitter.com/brysonbort](https://twitter.com/brysonbort)

## **SpeakerBio:**Gadi Evron

Gadi Evron is the Innovation Domain Lead at Citi and co-wrote the post-mortem for "the first Internet war", in Estonia (2007).

Twitter: [@https://twitter.com/gadievron](https://twitter.com/gadievron)

## **Description:**

It's been a long 12 years since the last time an Internet Wars panel was held at DEF CON, in that time a lot has changed, and a lot has not. This panel will bring together representatives from multiple industries and with a breadth of experiences discuss current trends and topics in internet security and the way those are playing out in both the cyber and the physical realm.

This discussion will start with an introductory presentation on some of the latest trends in digital security, threat intel, disinformation, and APTs. Further we will be discussing how cyber threats are being weaponized in the Russian attacks on Ukraine. From there we'll move into questions and answers from the audience. Panelists will accept questions on any subject related to the threat landscape, IoT and ICS threats, internet warfare and will discuss what we expect is coming and how we, as an industry, can best deal with it.

---

[Return to Index](#) - Add to



- ics [Calendar](#) file

---

## **LPV - Friday - 13:00-13:30 PDT**

---

**Title:** Intro to Lockpicking

**When:** Friday, Aug 12, 13:00 - 13:30 PDT

**Where:** Caesars Forum - Summit 203-204, 235

## **SpeakerBio:**TOOOL

No BIO available

## 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



- ics [Calendar](#) file

---

## LPV - Friday - 10:15-10:45 PDT

---

**Title:** Intro to Lockpicking

**When:** Friday, Aug 12, 10:15 - 10:45 PDT

**Where:** Caesars Forum - Summit 203-204, 235

**SpeakerBio:**TOOOL

No BIO available

## 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



- ics [Calendar](#) file

---

## LPV - Friday - 16:00-16:30 PDT

---

**Title:** Intro to Lockpicking

**When:** Friday, Aug 12, 16:00 - 16:30 PDT

**Where:** Caesars Forum - Summit 203-204, 235

**SpeakerBio:**TOOOL

No BIO available

## 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



- ics [Calendar](#) file

---

## LPV - Saturday - 10:15-10:45 PDT

---

**Title:** Intro to Lockpicking

**When:** Saturday, Aug 13, 10:15 - 10:45 PDT

**Where:** Caesars Forum - Summit 203-204, 235

**SpeakerBio:**TOOOL

No BIO available

### 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 Calendar](#) - ics [Calendar](#) file

---

## LPV - Sunday - 10:15-10:45 PDT

---

**Title:** Intro to Lockpicking

**When:** Sunday, Aug 14, 10:15 - 10:45 PDT

**Where:** Caesars Forum - Summit 203-204, 235

**SpeakerBio:**TOOOL

No BIO available

### 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 Calendar](#) - ics [Calendar](#) file

---

## LPV - Saturday - 13:00-13:30 PDT

---

**Title:** Intro to Lockpicking

**When:** Saturday, Aug 13, 13:00 - 13:30 PDT

**Where:** Caesars Forum - Summit 203-204, 235

**SpeakerBio:**TOOOL

No BIO available

### 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 Calendar](#) - ics [Calendar](#) file

---

## LPV - Sunday - 13:00-13:30 PDT

---

**Title:** Intro to Lockpicking

**When:** Sunday, Aug 14, 13:00 - 13:30 PDT

**Where:** Caesars Forum - Summit 203-204, 235

**SpeakerBio:**TOOOL

No BIO available

### 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 Calendar](#) - ics [Calendar](#) file

---

## LPV - Saturday - 16:00-16:30 PDT

---

**Title:** Intro to Lockpicking

**When:** Saturday, Aug 13, 16:00 - 16:30 PDT

**Where:** Caesars Forum - Summit 203-204, 235

**SpeakerBio:**TOOOL

No BIO available

### 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 Calendar](#) - ics [Calendar](#) file

---

## CPV - Saturday - 11:00-11:30 PDT

---

**Title:** Introducing the Abusability Testing Framework (V1)

**When:** Saturday, Aug 13, 11:00 - 11:30 PDT

**Where:** Flamingo - Vista Ballroom

**Speakers:**Nicole Chi,Ji Su Yoo,Avi Zajac

**SpeakerBio:**Nicole Chi

Nicole Chi (@nchisays, she/her) is currently a product manager working on Trust & Safety features, and the creator of Algorithm Unwrapped, a project to help people make sense of algorithmic content harms. She formerly worked on environmental restoration products and digital capacity building for nonprofits.

Twitter: [@https://twitter.com/nchisays](https://twitter.com/nchisays)

**SpeakerBio:**Ji Su Yoo

Ji Su (@JiSuYoo1, she/her) is a PhD at UC Berkeley's School of Information and former researcher at the Harvard Data Privacy Lab.

Twitter: <https://twitter.com/JiSuYoo1>

### **SpeakerBio:**Avi Zajac

Avi (@\_llzes, Avi/they/he) is a privacy-focused hacker. They love rabbits, cheesecake, and cute things like privacy and security, locksport, cryptography. They builds mission-driven products; help individuals and organisations protect their privacy and safety; and enjoy making and breaking things for a more equitable world.

### **Description:**

Are you concerned about how your products may be used for harm: intentionally or unintentionally? We introduce core concepts of abusability testing from our first public framework release, so you can walk away with an understanding of what abusability testing is, understand how to incorporate it, and learn how to alleviate harm in your own products with actionable steps.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## **ASV - Saturday - 12:00-12:50 PDT**

---

**Title:** Introduction to Aircraft Networks and Security Design Considerations

**When:** Saturday, Aug 13, 12:00 - 12:50 PDT

**Where:** Caesars Forum - Forum 112-117

### **SpeakerBio:**Sean Sullivan , Chief Engineer for Cabin, Network Systems and Product Security

Sean Sullivan is the Boeing Commercial Airplanes Chief Engineer for Cabin, Network Systems and Product Security. Sullivan held multiple positions in Boeing over a career of 34 years.

### **Description:**

How is a commercial aircraft's avionics network designed? How is an aircraft architecture integrated with an avionics network? Come learn about complexity of the aviation systems environment, aircraft design security requirements, design assurance levels, and lastly dive deep from a cyber perspective into an aircraft environment we are all familiar with: the passenger cabin.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## **WS - Thursday - 15:00-18:59 PDT**

---

**Title:** Introduction to Azure Security

**When:** Thursday, Aug 11, 15:00 - 18:59 PDT

**Where:** Harrah's - Silver

**Speakers:**Nishant Sharma,Jeswin Mathai

### **SpeakerBio:**Nishant Sharma , Security Research Manager

Nishant Sharma is a Security Research Manager at INE, where he manages the development of next-generation on-demand labs. Before INE, he worked as R&D Head of Pentester Academy (Acquired by INE), where he led a team of developers/researchers to create content and platform features for AttackDefense. He has also developed multiple gadgets for WiFi pentesting/monitoring such as WiMonitor, WiNX, and WiMini. With over 9+ years of experience in development and

content creation, he has conducted trainings/workshops at Blackhat Asia/USA, HITB Amsterdam/Singapore, OWASP NZ day, and DEFCON USA villages. He has presented/published his work at Blackhat USA/Asia Arsenal, DEFCON USA/China, Wireless Village, Packet Village and IoT village. He has also conducted WiFi Pentesting training at Blackhat USA 2019, 2021. He had started his career as a firmware developer at Mojo Networks (Acquired by Arista) where he worked on new features for the enterprise-grade WiFi APs and maintenance of state-of-the-art WIPS. He has a Master degree in Information Security from IIIT Delhi. He has also published peer-reviewed academic research on HMAC security. His areas of interest include WiFi, Azure, and Container security.

### **SpeakerBio:**Jeswin Mathai , Senior Security Researcher

Jeswin Mathai is a Senior Security Researcher at INE. Prior to joining INE, He was working as a senior security researcher at Pentester Academy (Acquired by INE). At Pentester Academy, he was also part of the platform engineering team who was responsible for managing the whole lab infrastructure. He has published his work at DEFCON China, RootCon, Blackhat Arsenal, and Demo labs (DEFCON). He has also been a co-trainer in classroom trainings conducted at Black Hat Asia, HITB, RootCon, OWASP NZ Day. He has a Bachelor degree from IIIT Bhubaneswar. He was the team lead at InfoSec Society IIIT Bhubaneswar in association with CDAC and ISEA, which performed security auditing of government portals, conducted awareness workshops for government institutions. His area of interest includes Cloud Security, Container Security, and Web Application Security.

### **Description:**

In recent times, Azure has become one of the dominant cloud service providers. Most enterprises today have some infrastructure if not all deployed on the cloud and attackers are constantly on the hunt for finding a way into the infrastructure.

Among the recent cloud hacks, around 97 percent are due to misconfigurations and various surveys suggest that in most cases, people were not aware of how misconfiguration can happen in various circumstances. Azure security is a mammoth in itself and a lot of people struggle in getting started with it, for the same reason many cloud administrators and developers are not aware of how misconfigurations and vulnerable applications can be leveraged to get a foothold on the account.

This workshop is a power course for Azure security, we will first cover the fundamentals and building blocks of Azure then we will take a look at the threatscape and attack vectors.

#### Materials

A laptop with the latest web browser and network connectivity A Kali VM (Virtual Box, VMWare, WSL)

#### Prereq

Basic knowledge of Linux and Networking

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## **WS - Friday - 10:00-13:59 PDT**

---

**Title:** Introduction to Cryptographic Attacks

**When:** Friday, Aug 12, 10:00 - 13:59 PDT

**Where:** Harrah's - Ely

### **SpeakerBio:**Matt Cheung , Hacker

Matt Cheung started developing his interest in cryptography during an internship in 2011. He worked on implementation of a secure multi-party protocol by adding elliptic curve support to an existing secure text pattern matching protocol.

Implementation weaknesses were not a priority and this concerned Matt. This concern prompted him to learn about cryptographic attacks from Dan Boneh's crypto 1 course offered on Coursera and the Matasano/cryptopals challenges. From this experience he has given workshops at the Boston Application Security Conference, BSidesLV, DEF CON, and the Crypto and Privacy Village.

## Description:

Using cryptography is often a subtle practice and mistakes can result in significant vulnerabilities. This workshop will cover many of these vulnerabilities which have shown up in the real world, including CVE-2020-0601. This will be a hands-on workshop where you will implement the attacks after each one is explained. I will provide a VM with Python dependencies and skeleton code included so you can focus on implementing the attack. A good way to determine if this workshop is for you is to look at the challenges at [cryptopals.com](http://cryptopals.com) and see if those look interesting, but you could use in person help understanding the attacks. While not a strict subset of those challenges, there is significant overlap.

### Materials

A laptop with VMWare or VirtualBox installed and capable of running a VM.

### Prereq

Students should be comfortable with modular arithmetic and the properties of XOR. Experience in Python or other similar language will be a plus.

[Return to Index](#) - Add to



- ics [Calendar file](#)

## WS - Thursday - 15:00-18:59 PDT

**Title:** Introduction to Software Defined Radios and RF Hacking

**When:** Thursday, Aug 11, 15:00 - 18:59 PDT

**Where:** Harrah's - Elko

### SpeakerBio:

Rich , Research Scientist  
Rich currently works as a research scientist focusing on radio communications and digital signals processing applications. Before making the jump to research, he was a RF engineer and embedded software developer working on prototype radio systems and DSP tools. He is passionate about radios and wireless technology and will happily talk for hours on the subject.

## Description:

This class is a beginner's introduction to practical Software Defined Radio (SDR) applications and development with an emphasis on hands-on learning. If you have ever been curious about the invisible world of radio waves and signals all around you, but didn't know where to begin, then this workshop is for you. Students can expect to learn about basic RF theory and SDR architecture before moving on to hands-on development with real radios. The instructor will guide students through progressively more complicated RF concepts and waveforms, culminating in a small capstone exercise. For this workshop, you must provide your own laptop and SDR. You can either purchase a RTL-SDR dongle kit which includes an antenna, small tripod, and a receive-only USB SDR for this class beforehand and bring it to the conference, or use a commercial SDR you already own. VMs will be made available to students to download before class, along with an OS setup guide for those that prefer a bare-metal install. The VM/OS will have all the required drivers and frameworks to interface with the radio hardware. My intent for this class is to lower the barrier of entry associated with RF topics, and for that reason I would like to emphasize that the workshop is geared toward complete beginner students with no prior experience working with SDRs; DEF CON attendees who already have experience with SDRs will likely find this course too simple.

### Materials

Students will need to come with the following: A laptop capable of running an Ubuntu VM (or an install of Ubuntu).

The VM/OS installation guide will be given out before Defcon. Digital Signals Processing is typically very computationally intensive, so I recommend a laptop with a 4 core processor and 8GB of RAM.

A Software Defined Radio, as this workshop is bring-your-own-device. I highly recommend a RTL2832 chip based kit that comes with a USB-powered SDR and an antenna mount. Two brands to consider are RTL-SDR and Nooelec. They are essentially the same, and I would pick whatever SDR is in stock at the time. Make sure to pick the kit that comes with the antenna accessories and not just the USB dongle. It should be between \$40 to \$50 USD:

<https://www rtl-sdr com/buy-rtl-sdr-dvb-t-dongles/> <https://www nooelec com/store/sdr/sdr-receivers/nesdr-smart.html>

If you already own a SDR (like a HackRF or one of the RTL-chip dongles) you can also use that. Just make sure to bring/buy an antenna.

Due to supply-chain issues, if you need to purchase a SDR for this workshop I highly recommend doing so ASAP.

#### Prereq

None, this is a workshop for complete beginners, although having some basic python knowledge would be a plus

---

[Return to Index](#) - Add to



- ics [Calendar](#) file

---

## IOTV - Sunday - 10:00-12:59 PDT

---

**Title:** IoT Village CTF Challenges

**When:** Sunday, Aug 14, 10:00 - 12:59 PDT

**Where:** Caesars Forum - Alliance 311, 320

#### Description:

Dive into hacking challenges with HTB at the IoT Village DEFCON 30 CTF. “House Edge” is a themed CTF challenge that aims to have the players travel through a mission inside a space casino with the final goal of accessing a safe box to retrieve its contents. Each challenge is a standalone and does not require to have solved any other challenges. That said, the content is structured in a specific order that helps facilitate the scenario, which at a high level can be broken down into the following side-tasks of the mission:

Gain access to the main security system to avoid being identified Steal RFID credentials of the reads in the open areas to gain access to restricted areas Disable the additional motion sensors in the restricted areas to avoid triggering an alarm Open a safe box and retrieve its contents.

---

[Return to Index](#) - Add to



- ics [Calendar](#) file

---

## IOTV - Saturday - 10:00-17:59 PDT

---

**Title:** IoT Village CTF Challenges

**When:** Saturday, Aug 13, 10:00 - 17:59 PDT

**Where:** Caesars Forum - Alliance 311, 320

#### Description:

Dive into hacking challenges with HTB at the IoT Village DEFCON 30 CTF. “House Edge” is a themed CTF challenge that aims to have the players travel through a mission inside a space casino with the final goal of accessing a safe box to retrieve its contents. Each challenge is a standalone and does not require to have solved any other challenges. That said, the content is structured in a specific order that helps facilitate the scenario, which at a high level can be broken down into the following side-tasks of the mission:

Gain access to the main security system to avoid being identified Steal RFID credentials of the reads in the open areas to gain access to restricted areas Disable the additional motion sensors in the restricted areas to avoid triggering an alarm Open a safe box and retrieve its contents.

---

[Return to Index](#) - Add to



- ics [Calendar](#) file

---

## IOTV - Friday - 10:00-17:59 PDT

---

**Title:** IoT Village CTF Challenges

**When:** Friday, Aug 12, 10:00 - 17:59 PDT

**Where:** Caesars Forum - Alliance 311, 320

### Description:

Dive into hacking challenges with HTB at the IoT Village DEFCON 30 CTF. “House Edge” is a themed CTF challenge that aims to have the players travel through a mission inside a space casino with the final goal of accessing a safe box to retrieve its contents. Each challenge is a standalone and does not require to have solved any other challenges. That said, the content is structured in a specific order that helps facilitate the scenario, which at a high level can be broken down into the following side-tasks of the mission:

Gain access to the main security system to avoid being identified Steal RFID credentials of the reads in the open areas to gain access to restricted areas Disable the additional motion sensors in the restricted areas to avoid triggering an alarm Open a safe box and retrieve its contents.

---

[Return to Index](#) - Add to



- ics [Calendar](#) file

---

## IOTV - Thursday - 00:00-15:59 PDT

---

**Title:** IoT Village CTF Creator's Contest

**When:** Thursday, Aug 11, 00:00 - 15:59 PDT

**Where:** Caesars Forum - Alliance 311, 320

### Description:

Got a cool new exploit on an IoT device and don't know what to do with it? The CTF Creators Contest is just the thing! Show us your research, put the device in the CTF and see if others can pop it. Oh, and did we mention the great prizes? Check out the IoT Village website for submission criteria <https://iotvillage.org/defcon.html#ctfCreatorsContest>

---

[Return to Index](#) - Add to



- ics [Calendar](#) file

---

## IOTV - Sunday - 10:00-12:59 PDT

---

**Title:** IoT Village CTF

**When:** Sunday, Aug 14, 10:00 - 12:59 PDT

**Where:** Caesars Forum - Alliance 311, 320

### Description:

The IoT Village CTF has over 30+ devices and challenges to find and exploit vulnerabilities in real IoT devices. Players, or teams up to 6 people, can register and compete against one another to win great prizes!. With an overall focus on real-life consequences, this year's CTF is the newest and best IoT Village CTF yet! The challenges will require creative thinking, knowledge in networking, and competency in exploit development to claim the top prize. Prizes will be awarded to the top 3 teams/players at the end of the event

## IOTV - Saturday - 10:00-17:59 PDT

---

**Title:** IoT Village CTF

**When:** Saturday, Aug 13, 10:00 - 17:59 PDT

**Where:** Caesars Forum - Alliance 311, 320

### Description:

The IoT Village CTF has over 30+ devices and challenges to find and exploit vulnerabilities in real IoT devices. Players, or teams up to 6 people, can register and compete against one another to win great prizes!. With an overall focus on real-life consequences, this year's CTF is the newest and best IoT Village CTF yet! The challenges will require creative thinking, knowledge in networking, and competency in exploit development to claim the top prize. Prizes will be awarded to the top 3 teams/players at the end of the event

---

## IOTV - Friday - 10:00-17:59 PDT

---

**Title:** IoT Village CTF

**When:** Friday, Aug 12, 10:00 - 17:59 PDT

**Where:** Caesars Forum - Alliance 311, 320

### Description:

The IoT Village CTF has over 30+ devices and challenges to find and exploit vulnerabilities in real IoT devices. Players, or teams up to 6 people, can register and compete against one another to win great prizes!. With an overall focus on real-life consequences, this year's CTF is the newest and best IoT Village CTF yet! The challenges will require creative thinking, knowledge in networking, and competency in exploit development to claim the top prize. Prizes will be awarded to the top 3 teams/players at the end of the event

---

## CPV - Saturday - 11:30-12:30 PDT

---

**Title:** Jailed By a Google Search Part 2: Abortion Surveillance in Post-Roe America

**When:** Saturday, Aug 13, 11:30 - 12:30 PDT

**Where:** Flamingo - Vista Ballroom

### SpeakerBio:

Kate Bertash

Kate is Director of the Digital Defense Fund, leading a team that provides technology and security resources and front-line support to the American abortion access movement. She brings together a background in nonprofit operations, technology startups, and public policy to this work. In her free time she designs fabrics that fool surveillance systems, and (full disclosure!) also helps out co-organizing the Crypto Privacy Village.

Twitter: [@https://twitter.com/KateRoseBee](https://twitter.com/KateRoseBee)

## Description:

The overturning of Roe v Wade brings with it grim implications not just for abortion access in America, but for all digital privacy rights. In this talk we revisit the threats to our privacy and encryption slipped into law and practice under the guise of “protecting life” that were first discussed in the 2018 talk “Jailed by a Google Search.” We will then examine the pervasive digital monitoring that in many ways creates an even more dangerous surveillance environment for pregnant people than before Roe’s 1973 landmark ruling (temporarily) federally legalizing abortion.

Today patients must navigate an ever-expanding interlocked web of digital data collection and anti-abortion misinformation, all while enduring the existing infrastructures of pregnancy surveillance in our medical and policing systems. By the end of this talk you’ll receive information on how to threat model issues that may come up in pursuing different safe abortion options, tips and strategies for digitally securing an abortion experience, and ways our privacy community can help take action.

---

[Return to Index](#) - Add to



- ics [Calendar](#) file

---

## DC - Friday - 18:00-18:45 PDT

---

**Title:** Killer Hertz

**When:** Friday, Aug 12, 18:00 - 18:45 PDT

**Where:** Caesars Forum - Forum 104-105, 135-136 (Track 1)

**SpeakerBio:** Chris Rock , Hacker

Chris Rock is a Cyber Mercenary who has worked in the Middle East, US and Asia for the last 30 years working for both government and private organizations. He is the Chief Information Security Officer and co-founder of SIEMONster.

Chris is an Information Security researcher who specializes on vulnerabilities in global systems. He presented at the largest hacking conference in the world, I Will Kill You? at DEFCON 23 in Las Vegas. Where he detailed how hackers could create fake people and kill them using vulnerabilities in the Birth and Death Registration systems around the world. Chris also presented How to Overthrow a Government? at DEFCON 24, working with the coup mercenary Simon Mann.

Chris is also the author of the Baby Harvest, a book based on criminals and terrorists using virtual babies and fake deaths for financing. He has also been invited to speak at TED global.

Twitter: [@https://twitter.com/chrisrockhacker](https://twitter.com/chrisrockhacker)

## Description:

Governments and the private sector around the world spend billions of dollars on Electronic Counter Measures (ECMs) which include jamming technologies. These jammers are used by police departments to disrupt criminal communication operations as well as in prisons to disrupt prisoners using smuggled in cell phones. The military use jammers to disrupt radar communications, prevent remote IEDs from triggering and radio communications. The private sector use jammers to disrupt espionage in the board room and to protect VIPs from RC-IEDs.

What if there was a way of communicating that was immune to jammers without knowing the point of origin. A way of communicating at short to medium distances, an Electronic Counter Countermeasure ECCM to the jammer.

Using a custom-built Tx/Rx, I will use the earth's crust to generate a H-field Near Field Communication (NFC) channel spanning 1-11km away in the sub 9 kHz range to communicate encrypted messages in a jammed environment.

---

[Return to Index](#) - Add to



- ics [Calendar](#) file

---

## CLV - Saturday - 15:00-16:59 PDT

---

**Title:** KQL Kung Fu: Finding the Needle in the Haystack in Your Azure Environments

**When:** Saturday, Aug 13, 15:00 - 16:59 PDT

**Where:** Flamingo - Scenic Ballroom

**SpeakerBio:**Darwin Salazar

Darwin Salazar is a Product Detection Engineer @ Datadog. Formerly a medical device security practitioner and cloud security consulting for several Fortune 500s. Enjoys reading, working out, spending time with family and giving back to his community.

Twitter: [@https://twitter.com/darwnsm](https://twitter.com/darwnsm)

### Description:

Kusto Query Language (KQL) is Microsoft's proprietary query language and has many use cases in enterprise Azure environments including threat hunting, threat detection and discovering misconfigured assets. In this workshop, I'll be going over these use cases and teaching the attendee how to structure KQL queries to get insights about activity in their Azure environments via Microsoft Sentinel.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## DDV - Sunday - 10:00-10:59 PDT

---

**Title:** Last chance to pick up drives at the DDV

**When:** Sunday, Aug 14, 10:00 - 10:59 PDT

**Where:** Flamingo - Exec Conf Ctr - Lake Meade and Valley of Fire

### Description:

This is your last chance to pickup your drives whether they're finished or not. Get here before 11:00am on Sunday as any drives left behind are considered donations.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## BTV - Saturday - 17:00-17:59 PDT

---

**Title:** Latest and Greatest in Incident Response

**When:** Saturday, Aug 13, 17:00 - 17:59 PDT

**Where:** Flamingo - Savoy Ballroom - BTV Main Stage

**Speakers:**Lauren Proehl,plug,LitMoose,Jess,zr0

**SpeakerBio:**Lauren Proehl

Lauren is currently the Sr Manager of Global Cyber Defense at Marsh McLennan... which is a wordy way of saying she manages CTI, Threat Hunting, Security Automation, and SOC things. When she isn't in front of a screen, she is running long distances in the woods, cycling over gravel trails, or acquiring more cats in order to reach crazy cat lady status.

**SpeakerBio:**plug

No BIO available

### **SpeakerBio:**LitMoose

Moose (aka Heather) is a benevolent Principal Incident Response consultant with CrowdStrike. Moose leads cases globally specializing in c-level grief counseling, eCrime stomping, forensic dumpster diving, attacker evictions, and long sessions staring deeply into logs, code, and config files. Outside of IR, Moose is a mother of cats, fiddler, and lover of potatoes in all forms.

### **SpeakerBio:**Jess

No BIO available

### **SpeakerBio:**zr0

zr0 is currently a Sr. Consultant on the IBM X-Force IR team leading both reactive and proactive DFIR engagements. In his spare time, z\_r0 loves playing competitive tennis, and exploring new things to do in the city with his new wife!

### **Description:**

IR is constantly in motion, adversaries change tactics and techniques and so do Incident Responders. Come hear from IR professionals what they've been up to for the past year.

IR is constantly in motion, adversaries change tactics and techniques and so do Incident Responders. Come hear from IR professionals what they've been up to for the past year.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## **AIV - Friday - 15:00-15:50 PDT**

---

**Title:** LATMA - Lateral movement analyzer

**When:** Friday, Aug 12, 15:00 - 15:50 PDT

**Where:** Caesars Forum - Summit 228->236

### **SpeakerBio:**Gal Sadeh

No BIO available

### **Description:**

Lateral movement is the stage in which attackers spread in networks following initial access. so far, reliable detections of lateral movement attacks from a given set of authentications is an unaddressed challenge. This talk will present a new online algorithm for detecting lateral movement attacks which provides one false positive a day, 30 times better than the state-of-the-art algorithms. Our algorithm was trained and tested on data from more than 20 different enterprise environments. The detection method combines domain knowledge, practical machine learning and algorithmic tools. In addition, we will present the offline tool LATMA which collects authentication AD logs, finds suspected lateral movement based on our algorithm and visualises the results. We will explain how to analyse lateral movement attacks using LATMA's visualisations and demonstrate it.

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## **SOC - Friday - 18:00-17:59 PDT**

---

**Title:** Lawyers Meet

**When:** Friday, Aug 12, 18:00 - 17:59 PDT

**Where:** Harrah's - Parlor D & The Veranda

## 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



- ics [Calendar](#) file

## DC - Friday - 14:30-15:15 PDT

**Title:** Leak The Planet: Veritatem cognoscere non pereat mundus

**When:** Friday, Aug 12, 14:30 - 15:15 PDT

**Where:** Caesars Forum - Forum 106-110, 138-139 (Track 2)

**Speakers:**Xan North,Emma Best

**SpeakerBio:**Xan North , Distributed Denial of Secrets

Xan North is a member of Distributed Denial of Secrets, a 501(c)(3) transparency non-profit sometimes referred to as a successor to WikiLeaks which has published leaks from over 50 countries. They have worked extensively in antifascist, anti-racist, and pro-choice activism and previously ran the Jeremy Hammond Support Committee for seven years and provided prisoner support to other associates of Anonymous.

Twitter: [@https://twitter.com/brazendyke](https://twitter.com/brazendyke)

**SpeakerBio:**Emma Best , Distributed Denial of Secrets

Emma Best is the co-founder of Distributed Denial of Secrets, a 501(c)(3) transparency non-profit sometimes referred to as a successor to WikiLeaks which has published leaks from over 50 countries. Previously, she has filed thousands of Freedom of Information Act (FOIA) requests, helped push the Central Intelligence Agency to publish 13 million pages of declassified files online, and written hundreds of articles. More importantly, she's the proud mom of two cats, a human and many Pokémon.

Twitter: [@https://twitter.com/NatSecGeek](https://twitter.com/NatSecGeek)

## Description:

As leaks become more prevalent, they come from an increasing variety of sources: from data that simply isn't secured, to insiders, to hacktivists, and even occasional state-actors (both covert and overt). Often treated as a threat, when handled responsibly leaks are a necessary part of the ecosystem of a healthy and free society and economy. In spite of prosecutors' love of prosecution, the eternal fixation with Fear, Uncertainty and Doubt and DDoSecrets' apocalyptic motto, leaks won't destroy the world - they can only save it.

In this presentation, we'll discuss the necessity and evolution of leaks, and how various types of leaks and sources can offer different sorts of revelations. We'll then explore how we can responsibly handle different types of leaks even during volatile and politically charged situations, as well as past failures.

We'll also debunk the myth that hacktivism is just a cover for state actors by exploring examples of entities with state ties and how they were identified, as well as how both hacktivists and state actors have been misidentified or mishandled in the past.

Finally, we'll discuss some of the lessons activists, newsrooms and governments can learn from the last decade, and where we should collectively go from here.

[Return to Index](#) - Add to



- ics [Calendar](#) file

**Title:** Lend me your IR's!**When:** Friday, Aug 12, 14:15 - 15:15 PDT**Where:** Virtual - BlueTeam Village - Talks**SpeakerBio:**Matt Scheurer

Matt Scheurer is a show host for the ThreatReel Podcast, and also works as an Assistant Vice President of Computer Security and Incident Response in a large enterprise environment. Matt has many years of hands-on technical experience, including Digital Forensics and Incident Response (DFIR). He volunteers as a "Hacking is NOT a Crime" Advocate and as a technical mentor for the Women's Security Alliance (WomSA). Matt is a 2019 comSpark "Rising Tech Stars Award" winner, and has presented on numerous Information Security topics at many technology meetup groups and prominent Information Security conferences across the country.

**Description:**

This is a fun technical talk covering three of my favorite security investigations as an Incident Response professional. The presentation features demoed reenactments of actual real-world attacks. I showcase both the attacker side as well as the investigation side of these security incidents. I show and talk through example source code and explain how each of the attacks work. I then flip these scenarios around by explaining how to use numerous free and open-source tools to investigate those same security incidents. Each scenario is closed by covering the follow-up remediation steps.

Protecting systems and networks as a tech defender means withstanding a constant barrage of unsophisticated attacks from automated tools, botnets, crawlers, exploit kits, phish kits, and script kiddies; oh my! Occasionally, we encounter attacks worthy of style points for creativity or new twists on old attack techniques. This talk features demoed reenactments from some advanced attacks investigated by the presenter. The demos showcase technical deep dives of the underpinnings from both the attacker and investigator sides of these attacks. Attendee key takeaways are strategies, freely available tools, and techniques helpful during incident response investigations.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

**DC - Sunday - 13:00-13:45 PDT****Title:** Less SmartScreen More Caffeine – ClickOnce (Ab)Use for Trusted Code Execution**When:** Sunday, Aug 14, 13:00 - 13:45 PDT**Where:** Caesars Forum - Forum 104-105, 135-136 (Track 1)**Speakers:**Nick Powers,Steven Flores**SpeakerBio:**Nick Powers , Consultant at SpecterOps

Nick Powers is an operator and red teamer at SpecterOps. He has experience with providing, as well as leading, pentest and red team service offerings for a large number of fortune 500 companies. Prior to offensive security, Nick gained security and consulting experience while offering compliance-based gap assessments and vulnerability audits. With a career focused on offensive security, his interests and prior research focuses have included initial access techniques, evasive Windows code execution, and the application of alternate C2 and data exfiltration channels.

Twitter: [@https://twitter.com/zyn3rgy](https://twitter.com/zyn3rgy)

**SpeakerBio:**Steven Flores , Senior Consultant at SpecterOps

Steven Flores is an experienced red team operator and former Marine. Over the years Steven has performed engagements against organizations of varying sizes in industries that include financial, healthcare, legal, and government. Steven enjoys learning new tradecraft and developing tools used during red team engagements. Steven has developed several commonly

used red team tools such as SharpRDP, SharpMove, and SharpStay.

Twitter: <https://twitter.com/0xthirteen>

## Description:

Initial access payloads have historically had limited methods that work seamlessly in phishing campaigns and can maintain a level of evasion. This payload category has been dominated by Microsoft Office types, but as recent news has shown, the lifespan of even this technique is shortening. A vehicle for payload delivery that has been greatly overlooked for initial access is ClickOnce. ClickOnce is very versatile and has a lot of opportunities for maintaining a level of evasion and obfuscation. In this talk we'll cover methods of bypassing Windows controls such as SmartScreen, application whitelisting, and trusted code abuses with ClickOnce applications. Additionally, we'll discuss methods of turning regular signed or high reputation .NET assemblies into weaponized ClickOnce deployments. This will result in circumvention of common security controls and extend the value of ClickOnce in the offensive use case. Finally, we'll discuss delivery mechanisms to increase the overall legitimacy of ClickOnce application deployment in phishing campaigns. This talk can bring to attention the power of ClickOnce applications and code execution techniques that are not commonly used.

---

[Return to Index](#) - Add to



- ics [Calendar](#) file

---

## DC - Friday - 17:00-17:45 PDT

---

**Title:** Let's Dance in the Cache - Destabilizing Hash Table on Microsoft IIS

**When:** Friday, Aug 12, 17:00 - 17:45 PDT

**Where:** Caesars Forum - Academy 401-410, 421 (Track 3)

**SpeakerBio:** Orange Tsai , Principal Security Researcher of DEVCore

Cheng-Da Tsai, aka Orange Tsai, is the principal security researcher of DEVCore and the core member of CHROOT security group in Taiwan. He is also the champion and got the "Master of Pwn" title in Pwn2Own 2021. In addition, Orange has spoken at several top conferences such as Black Hat USA/ASIA, DEF CON, HITCON, HITB GSEC/AMS, CODE BLUE, POC, and WooYun!

Currently, Orange is a 0day researcher focusing on web/application security. His research got not only the Pwnie Awards winner for "Best Server-Side Bug" of 2019/2021 but also 1st place in "Top 10 Web Hacking Techniques" of 2017/2018. Orange also enjoys bug bounties in his free time. He is enthusiastic about the RCE bugs and uncovered RCEs in numerous vendors such as Twitter, Facebook, Uber, Apple, GitHub, Amazon, etc. You can find him on Twitter @orange\_8361 and blog <http://blog.orange.tw/>

Twitter: [https://twitter.com/orange\\_8361](https://twitter.com/orange_8361)

## Description:

Hash Table, as the most fundamental Data Structure in Computer Science, is extensively applied in Software Architecture to store data in an associative manner. However, its architecture makes it prone to Collision Attacks. To deal with this problem, 25 years ago, Microsoft designed its own Dynamic Hashing algorithm and applied it everywhere in IIS, the Web Server from Microsoft, to serve various data from HTTP Stack. As Hash Table is everywhere, isn't the design from Microsoft worth scrutinizing?

We dive into IIS internals through months of Reverse-Engineering efforts to examine both the Hash Table implementation and the use of Hash Table algorithms. Several types of attacks are proposed and uncovered in our research, including (1) A specially designed Zero-Hash Flooding Attack against Microsoft's self-implemented algorithm. (2) A Cache Poisoning Attack based on the inconsistency between Hash-Keys. (3) An unusual Authentication Bypass based on a hash collision.

By understanding this talk, the audience won't be surprised why we can destabilize the Hash Table easily. The audience will also learn how we explore the IIS internals and will be surprised by our results. These results could not only make a default

installed IIS Server hang with 100% CPU but also modify arbitrary HTTP responses through crafted HTTP request. Moreover, we'll demonstrate how we bypass the authentication requirement with a single, crafted password by colliding the identity cache!

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## DC - Saturday - 10:00-10:45 PDT

---

**Title:** Literal Self-Pwning: Why Patients - and Their Advocates - Should Be Encouraged to Hack, Improve, and Mod Med Tech

**When:** Saturday, Aug 13, 10:00 - 10:45 PDT

**Where:** Caesars Forum - Alliance 301-309, 321 (Track 4)

**Speakers:**Christian "quaddi" Dameff MD,Jeff "r3plicant" Tully MD,Cory Doctorow

**SpeakerBio:**Christian "quaddi" Dameff MD , Emergency Medicine Physician & Hacker at The University of California San Diego

Christian (quaddi) Dameff MD is an Assistant Professor of Emergency Medicine, Biomedical Informatics, and Computer Science (Affiliate) at the University of California San Diego. He is also a hacker, former open capture the flag champion, and prior DEF CON/RSA/Blackhat/HIMSS speaker. Published works include topics such as therapeutic hypothermia after cardiac arrest, novel drug targets for myocardial infarction patients, and other Emergency Medicine related works. Published security research topics including hacking critical healthcare infrastructure, medical devices and the effects of malware on patient care. This is his eighteenth DEF CON.

Twitter: [@https://twitter.com/CDameffMD](https://twitter.com/CDameffMD)

**SpeakerBio:**Jeff "r3plicant" Tully MD , Anesthesiologist at The University of California San Diego

Jeff (r3plicant) Tully is a security researcher with an interest in understanding the ever-growing intersections between healthcare and technology. His day job focuses primarily on the delivery of oxygen to tissues.

Twitter: [@https://twitter.com/JeffTullyMD](https://twitter.com/JeffTullyMD)

**SpeakerBio:**Cory Doctorow , Science fiction author, activist and journalist

Cory Doctorow (raphound.com) is a science fiction author, activist and journalist. He is the author of many books, most recently RADICALIZED and WALKAWAY, science fiction for adults, IN REAL LIFE, a graphic novel; INFORMATION DOESN'T WANT TO BE FREE, a book about earning a living in the Internet age, and HOMELAND, a YA sequel to LITTLE BROTHER. His next book is ATTACK SURFACE.

Twitter: [@https://twitter.com/doctorow](https://twitter.com/doctorow)

### Description:

What do Apple, John Deere and Wahl Shavers have in common with med-tech companies? They all insist that if you were able to mod their stuff, you would kill yourself and/or someone else... and they've all demonstrated, time and again, that they are unfit to have the final say over how the tools you depend on should work. As right to repair and other interoperability movements gain prominence, med-tech wants us to think that it's too life-or-death for modding. We think that med-tech is too life-or-death NOT to be open, accountable and configurable by the people who depend on it. Hear two hacker doctors and a tech activist talk about who's on the right side of history and how the people on the wrong side of history are trying to turn you into a walking inkjet printer, locked into an app store.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## DC - Saturday - 16:00-16:45 PDT

---

**Title:** Low Code High Risk: Enterprise Domination via Low Code Abuse

**When:** Saturday, Aug 13, 16:00 - 16:45 PDT

**Where:** Caesars Forum - Academy 401-410, 421 (Track 3)

**SpeakerBio:** Michael Bargury , Co-Founder and CTO, Zenity.io

Michael Bargury is the Co-Founder and CTO of Zenity, where he helps companies secure their low-code/no-code apps. In the past, he headed security product efforts at Azure focused on IoT, APIs and IaC. Michael is passionate about all things related to cloud, SaaS and low-code security, and spends his time finding ways they could go wrong. He also leads the OWASP low-code security project and writes about it on DarkReading.

Twitter: [@https://twitter.com/mbrg0](https://twitter.com/mbrg0)

### Description:

Why focus on heavily guarded crown jewels when you can dominate an organization through its shadow IT?

Low-Code applications have become a reality in the enterprise, with surveys showing that most enterprise apps are now built outside of IT, with lacking security practices. Unsurprisingly, attackers have figured out ways to leverage these platforms for their gain.

In this talk, we demonstrate a host of attack techniques found in the wild, where enterprise No-Code platforms are leveraged and abused for every step in the cyber killchain. You will learn how attackers perform an account takeover by making the user simply click a link, move laterally and escalate privileges with zero network traffic, leave behind an untraceable backdoor, and automate data exfiltration, to name a few capabilities. All capabilities will be demonstrated with POCs, and their source code will be shared.

Next, we will drop two isolation-breaking vulnerabilities that allow privilege escalation and cross-tenant access. We will explain how these vulnerabilities were discovered and assess their pre-discovery impact.

Finally, we will introduce an open-source recon tool that identifies opportunities for lateral movement and privilege escalation through low-code platforms.

---

[Return to Index](#) - Add to



- ics [Calendar](#) file

---

## DC - Friday - 15:00-15:45 PDT

---

**Title:** LSASS Shtinkering: Abusing Windows Error Reporting to Dump LSASS

**When:** Friday, Aug 12, 15:00 - 15:45 PDT

**Where:** Caesars Forum - Academy 401-410, 421 (Track 3)

**Speakers:** Asaf Gilboa, Ron Ben Yitzhak

**SpeakerBio:** Asaf Gilboa , Security Researcher, Deep Instinct

Asaf and Ron are Security Researchers at Deep Instinct where they both work on developing new defense capabilities based on research and understanding and novel attack techniques and vectors. After serving for several years in the advanced technological cyber units of the IDF, Asaf and Ron gained experience in the multiple aspects of technical cyber-security work including forensics, incident response, development, reverse engineering and malware research.

**SpeakerBio:** Ron Ben Yitzhak

Asaf Gilboa and Ron Ben Yitzhak

Asaf and Ron are Security Researchers at Deep Instinct where they both work on developing new defense capabilities based on research and understanding and novel attack techniques and vectors. After serving for several years in the advanced technological cyber units of the IDF, Asaf and Ron gained experience in the multiple aspects of technical cyber-security work including forensics, incident response, development, reverse engineering and malware research.

## Description:

This presentation will show a new method of dumping LSASS that bypasses current EDR defenses without using a vulnerability but by abusing a built-in mechanism in the Windows environment which is the WER (Windows Error Reporting) service.

WER is a built-in system in Windows designed to gather information about software crashes. One of its main features is producing a memory dump of crashing user-mode processes for further analysis.

We will present in detail and demo a new attack vector for dumping LSASS, which we dubbed LSASS Shtinkering, by manually reporting an exception to WER on the LSASS process without crashing it. The technique can also be used to dump the memory of any other process of interest on the system.

This attack can bypass defenses that wrongfully assume that a memory dump generated from the WER service is always a benign or non-attacker triggered activity.

The talk will take the audience through the steps and approach of how we reverse-engineered the WER dumping process, the challenges we found along the way, as well as how we have managed to solve them.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## AIV - Friday - 13:00-13:50 PDT

---

**Title:** Machine Learning Security Evasion Competition Launch

**When:** Friday, Aug 12, 13:00 - 13:50 PDT

**Where:** Caesars Forum - Summit 228->236

**SpeakerBio:** Hyrum Anderson

No BIO available

## Description:

Calling ML practitioners and security researchers to compete in two competitions. Returning to AI Village is the ML Security Evasion Competition—with new twists for the offense-minded contestant. New to AI Village this year is the ML Model Attribution Challenge for those interested in defense and compliance. There are multiple ways to win in each competition, with first place prizes at \$3000 USD, honorable mention prizes at \$1500 USD, and multiple student awards also valued at \$1500 USD. In all, we'll be giving away up to \$20K USD divided amongst up to 9 top contestants. The challenges begin now!

In the ML Security Evasion Competition (<https://mlsec.io>), you are an attacker attempting to bypass HTML antiphishing models, and biometric face recognition models in two separate challenges. Modify HTML or image samples in a way to fool the models hosted by the competition sponsors. Visit <https://mlsec.io> to register, participate, submit and potentially win. You have 6 weeks to submit (Sep 23, 2022).

In the ML Model Attribution Challenge (<https://mlmac.io>), you take the role of an adjudicator, where you must determine which base model has been used for several fine-tuned generative models hosted by the competition sponsors. Query the models to investigate what might be under the hood. Students are especially encouraged to apply, with additional travel awards given to top student submissions to present results at <https://camlis.org>. Visit <https://mlmac.io> to register, participate,

submit and potentially win. You have 4 weeks to submit (Sep 9, 2022).

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## CLV - Friday - 10:50-11:30 PDT

---

**Title:** Making the most of Microsoft cloud bug bounty programs: How I made in \$65,000 USD in bounties in 2021

**When:** Friday, Aug 12, 10:50 - 11:30 PDT

**Where:** Flamingo - Scenic Ballroom

### **SpeakerBio:**Nestori Syynimaa

Dr Nestori Syynimaa (@DrAzureAD) is one of the leading Azure AD / M365 security experts globally and the developer of the AADInternals toolkit. For over a decade, he has worked with Microsoft cloud services and was awarded Microsoft Most Valuable Security Researcher for 2021. Currently, Dr Syynimaa works as a Senior Principal Security Researcher for Secureworks Counter Threat Unit and hunts for vulnerabilities full time. He has spoken at many international scientific and professional conferences, including IEEE TrustCom, Black Hat Arsenal USA and Europe, RSA Conference, and TROOPERS. Twitter: [@https://twitter.com/DrAzureAD](https://twitter.com/DrAzureAD)

### **Description:**

Microsoft Cloud bug bounty programs are one of the most well-paid programs, including Microsoft Identity program. This program covers cloud-related Elevation of Privilege vulnerabilities, having bounties up to \$100,000! But as all vulnerabilities are not worth 100k, it's good to know how to make most of the low-bounty vulnerabilities.

In this talk, I'll share my experiences on the Microsoft bounty programs from 2021, when I made \$65k in bounties with six vulnerabilities. I'll show how I turned a vulnerability initially categorized as 'by-design' to \$40k in bounties and how I tripled the initial \$5k bounty by reporting similar findings smartly.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## BTV - Saturday - 16:00-16:59 PDT

---

**Title:** Making Your SOC Suck Less

**When:** Saturday, Aug 13, 16:00 - 16:59 PDT

**Where:** Flamingo - Savoy Ballroom - BTV Main Stage

**Speakers:**Shawn Thomas,Carson Zimmerman,Sebastian Stein,Alissa Torres,Jackie Bow

### **SpeakerBio:**Shawn Thomas

Shawn is ex Incident Response consultant, SOC manager, and current Head of Incident Response at Yahoo!, a Paranoid by trade and title he has spent his career trying to find badness and protect users. Shawn has worked in or managed many SOC's across both the government, private sector, and MSSP space. He loves to teach and talk DFIR/Operations, volunteer at conferences, host podcasts, including Positively Blue Team and The Paranoids Podcast, and help run the DeadPixelSec discord community which is his infosec home.

### **SpeakerBio:**Carson Zimmerman

Carson Zimmerman has been working in cybersecurity for about 20 years. In his current role at Microsoft, he leads an investigations team responsible for defending the M365 platform and ecosystem. Previously at The MITRE Corporation, Carson specialized in cybersecurity operations center architecture, consulting, and engineering. In his early days at MITRE, Carson worked in roles ranging from CSOC tier 1 analysis, to secure systems design consulting, to vulnerability assessment.

### **SpeakerBio:**Sebastian Stein

Security Operations Leader from the "uber innovative" SF Bay Area (originally from Berlin) with 12y of security and 10y of infra experience. Currently defending a \$2B publicly traded pharmaceutical company. Security at scale is hard! And when everything is cobbled together with off-the-shelf software, it is almost impossible. Security teams always have everyone else's back and are absolutely allowed to fail.

### **SpeakerBio:**Alissa Torres

No BIO available

### **SpeakerBio:**Jackie Bow

A Jackie-of-all-trades, master of none, Jackie seems to be physically unable to stop returning to threat detection and response. Her 10 years in the industry have been spent in malware analysis, reverse engineering, and infrastructure and product security. She has been an analyst, engineer, and leader. Currently, she is focused on building out the threat detection and response program at Asana. She aspires to build teams that leave members better than they were found, technically AND mentally. She speaks and sometimes writes about burnout awareness and efforts to dismantle the gatekeeping of technical security roles.

### **Description:**

The Security Operations Center: is it really more than a place to go where dreams die? So many analysts feel that the soul-sucking march of awful false positive alerts will never end; there's no way to improve and they're in a dead end job. How can you turn your nightmare into something more bearable? Come join our panelists, four security analysts turned leaders, as they get grilled by our moderator in answering this question and more. By the end of this talk, you will gain a series of tips and tricks to take back to your SOC whether it's new or old, big or small, chaotic or calm. You will learn how to get the most from your individual experience, lift up your team around you, or at least recognize when it's time to run like mad.

The Security Operations Center: is it really more than a place to go where dreams die? So many analysts feel that there's no way to improve and they're in a dead end job. How can you turn your nightmare into something more bearable? By the end of this panel, you will gain a series of tips and tricks to take back to your SOC, you will learn how to get the most from your individual experience, lift up your team around you, or at least recognize when it's time to run like mad.

---

[Return to Index](#) - Add to



- ics [Calendar](#) file

---

### **BTV - Friday - 11:45-12:45 PDT**

---

**Title:** Malicious memory techniques on Windows and how to spot them

**When:** Friday, Aug 12, 11:45 - 12:45 PDT

**Where:** Virtual - BlueTeam Village - Talks

### **SpeakerBio:**Connor Morley

Connor Morley is a senior security researcher at WithSecure. A keen investigator of malicious TTP's, he enjoys experimenting and dissecting malicious tools to determine functionality and developing detection methodology. As a researcher and part time threat hunter he is experienced with traditional and 'in the wild' malicious actors' behaviour.

### **Description:**

My presentation will cover malicious memory techniques which will focus on the Windows operating system. These will span from relatively simple in-line hooking techniques used to jump to malicious code or circumvent legitimate code execution, all the way to manipulation of exception handling mechanisms. The talk will also cover information on problematic situations which occur when designing detection mechanisms for such activities in the real world where cost-balancing is required for resource management.

I will explain in-line hooking, Kernel patching (InfinityHook, Ghost\_in\_the\_logs), Heaven-Gate hooking and Vectored Exception Handler (VEH) manipulation techniques (FireWalker) and how they can be detected. In-line hooking and Heavens-Gate hooking involves the practice of manipulating the loaded memory of a module within a specific processes memory space. Kernel Patching involves injecting a hook into the Kernel memory space in order to provide a low level, high priority bypassing technique for malicious programs to circumvent ETW log publication via vulnerable kernel driver installation. VEH manipulation is the use of the high priority frameless exception mechanism in order to circumvent memory integrity checks, manipulate flow control and even run malicious shellcode. Detection for all these techniques will involve advancing from the explanation of its execution to the telemetry sources that can be leveraged for detection purposes. In all cases this involves the examination of volatile memory, however as each technique targets a different native functionality, the mechanisms required to analyze the memory differ greatly. The deviations can be relatively simple, but in some cases an understanding of undocumented mechanisms and structures is required to affect detection capability

Examination of un-tabled module function modifications will also provide insight into some of the difficulties involved in this detection development work. This section will provide the audience with a low level technical understanding of how these techniques are targeted, developed and used by malicious actors and some possible solutions for detection, with an explanation of the inherent caveats in such solutions (primarily around resource availability or accuracy trade-offs).

A full explanation on devised detection methodology and collectable telemetry will be provided for each malicious technique. This will cover the overall detection capabilities as well as exploring the low level mechanisms used to collect this data from the monitored system such as OP code heuristics and memory location attribution crossing CPU mode boundaries. Included in this explanation will be an explanation on issues encountered with collection, typically related to OS architecture choices, and how these can also be circumvented to enable effective monitoring.

Audience members should leave my presentation having a firm grasp on the fundamentals of all the techniques outlined and why attackers may choose to employ them in different scenarios. Along with a functional understanding of the malicious technique, the audience members will also be supplied with a working understanding of detection options for these techniques and clear examples of how monitoring can be deployed and integrated into their solutions.

Malicious actors are always trying to find new ways to avoid detection by evermore vigilant EDR systems and deploy their payloads. Over the years, the scope of techniques used has branched from relatively simplistic hash comparison and sandbox avoidance to low level log dodging and even direct circumvention of EDR telemetry acquisition. By examining some of the techniques used on Windows systems this talk will highlight the range of capabilities defensive operators are dealing with, how some can be detected and, in rare cases, the performance and false-positive obstacles in designing detection capability.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## BTW - Friday - 15:30-16:30 PDT

---

**Title:** Malware Hunting - Discovering techniques in PDF malicious

**When:** Friday, Aug 12, 15:30 - 16:30 PDT

**Where:** Virtual - BlueTeam Village - Talks

### SpeakerBio:Filipi Pires

I've been working as Security Researcher at Saporó, Cybersecurity Advocate at senhasegura, Snyk Ambassador, Application Security Specialist, Hacking is NOT a crime Advocate and RedTeam Village Contributor. I'm part of the Coordinator team from DCG5511(DEFCON Group São Paulo-Brazil), International Speakers in Security and New technologies events in many countries such as US, Canada, France, Spain, Germany, Poland, etc, I've been served as University Professor in 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) and Malware Analysis-Fundamentals(HackerSec).

## Description:

We'll walk through the structures of a PDF, analyzing each part of it, demonstrating how Threat Actors work in the inclusion of malicious components in the structures of the file, in addition to demonstrating the collection of IOC(Indicators of Attack) and how to build IOA(Indicators of Attack) for analysis by behavior, to anticipate new attacks. Demonstrating structures in the binaries as a PDF(header/ body/cross-reference table/trailer) and performing a comparison of malicious PDFs, explaining how each session works within a binary, what are the techniques used such as packers, obfuscation with JavaScript (PDF) and more, explaining too about some anti-disassembly techniques, demonstrating as a is the action of these malware's and where it would be possible to "include" a malicious code.

Demonstrate different kind of structures in the binaries as a PDF(header/ body/cross-reference table/trailer), explaining how each session works within a binary, what are the techniques used such as packers, obfuscation with JavaScript (PDF) and more

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## MIV - Saturday - 10:45-12:30 PDT

---

**Title:** Mass Disinformation Operations - How to detect and assess Ops with OSINT & SOCMINT tools and techniques

**When:** Saturday, Aug 13, 10:45 - 12:30 PDT

**Where:** Caesars Forum - Summit 221->236

### **SpeakerBio:**Paula González Nagore

Paula González Nagore is an Intelligence Analyst specialized in OSINT and SOCMINT investigations and Cyber Intelligence. She currently works in the private sector conducting Digital Footprint, Digital Surveillance and Competitive Intelligence investigations. She also collaborates with different public and educational institutions to investigate disinformation and its effects, as well as the digital tools that are used today to develop disinformation campaigns and fake news in digital media and social networks.

**Description:**No Description available

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## WS - Saturday - 10:00-13:59 PDT

---

**Title:** Master Class: Delivering a New Construct in Advanced Volatile Memory Analysis for Fun and Profit

**When:** Saturday, Aug 13, 10:00 - 13:59 PDT

**Where:** Harrah's - Ely

### **SpeakerBio:**Solomon Sonya , Director of Cyber Operations Training

Solomon Sonya (@Carpenter1010) is the Director of Cyber Operations Training at a large organization. He has a background in software development, malware analysis, covert channels, steganography, distributed computing, computer hacking, information protection paradigms, and cyber warfare. He received his Undergraduate Degree in Computer Science and has Master's degrees in Computer Science and Information System Engineering. Before becoming Director of Cyber Operations Training, he was a university Computer Science Assistant Professor of Computer Science and Research Director. Solomon's current research includes computer system exploitation, cyber threat intelligence, digital forensics, and data protection.

Solomon's previous keynote and conference engagements include: BlackHat USA, SecTor Canada, Hack in Paris, France, HackCon Norway, ICSIS – Toronto, ICORES Italy, BruCon Belgium, CyberCentral – Prague and Slovakia, Hack.Lu Luxembourg, Shmoocon DC, BotConf - France, DerbyCon Kentucky, SkyDogCon Tennessee, HackerHalted Georgia,

Day-Con Ohio, and TakeDownCon Connecticut, Maryland, and Alabama, AFCEA – Colorado Springs.

Twitter: [@https://twitter.com/Carpenter1010](https://twitter.com/Carpenter1010)

## Description:

Malware continues to advance in sophistication. Well-engineered malware can obfuscate itself from the user and the OS. Volatile memory is the unique structure malware cannot evade. I have engineered a new construct for memory analysis and a new open-source tool that automates memory analysis, correlation, and user-interaction to increase investigation accuracy, reduce analysis time and workload, and better detect malware presence from memory. This workshop introduces a new visualization construct that creates the ability to interact with memory analysis artifacts. We will cover how to conducted advanced memory analysis utilizing this brand new tool that will greatly enhance the analysis process. Additionally, we will learn how to use new Data XREF and System Manifest features in this workshop. Data XREF provides an index and memory context detailing how your search data is coupled with processes, modules, and events captured in memory. The System Manifest distills the analysis data to create a new memory analysis snapshot and precise identification of malicious artifacts detectable from malware execution especially useful for exploit dev and malware analysis! This talk is perfect if you have conducted memory analysis before and understand the pain it is to conduct this type of analysis by hand. In this workshop, we will work with a new revolutionary tool to automate, correlate, and enrich memory analysis saving you hours of analysis time. This work shop exposes participants to capture-the-flag memory analysis challenges utilizing the new Xavier Memory Analysis Framework and concludes with a culminating capstone exercise at the end. Participants will walk away with advanced memory analysis capabilities including how to recognize and handle various forms of advance code injection and rootkit hooking techniques from computer memory.

## Materials

Just a laptop with VirtualBox installed. I will provide the memory images with all tools configured ready for the workshop.

## Prereq

None

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## LPV - Friday - 11:00-11:30 PDT

---

**Title:** Medeco cam lock exploit "an old attack made new again"

**When:** Friday, Aug 12, 11:00 - 11:30 PDT

**Where:** Caesars Forum - Summit 203-204, 235

**SpeakerBio:**N thing

No BIO available

## Description:

Rethinking a 100 year old exploit. This talk will be describing and demonstrating an awesome attack on one of the most used high security locks in the country.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## BHV - Friday - 16:30-17:59 PDT

---

**Title:** Medical Device Hacking: A hands on introduction

**When:** Friday, Aug 12, 16:30 - 17:59 PDT

**Where:** Flamingo - Laughlin I,II,III

### **SpeakerBio:**Malcolm Galland

Malcolm is an Associate Director and the Embedded Device Vertical Lead at Protiviti. He regularly performs device security pentests in the Medical and Financial sectors.

### **Description:**

"A presentation about how easy hardware hacking is using a couple of over the counter medical devices to show how debug access, firmware reverse engineering, etc work in the embedded medical device pentesting world. Live demos on real products with a workshop to follow. "

---

[Return to Index](#) - Add to



- ics [Calendar](#) file

---

## **SOC - Friday - 17:00-19:59 PDT**

---

**Title:** Meet the Digital Lab at Consumer Reports

**When:** Friday, Aug 12, 17:00 - 19:59 PDT

**Where:** Caesars Forum - Accord Boardroom

### **Description:**

Consumer Reports Digital Lab is a team of hackers, technologists and advocates that break the products we use every day to identify vulnerabilities that harm consumers. Come meet CR's resident hackers and learn how you can hack alongside us. We'll be showcasing our work in IoT, VPNs, and data rights and asking you how we can better leverage our security testing and research to provoke industry change.

---

[Return to Index](#) - Add to



- ics [Calendar](#) file

---

## **SOC - Saturday - 20:00-21:59 PDT**

---

**Title:** Meet the EFF

**When:** Saturday, Aug 13, 20:00 - 21:59 PDT

**Where:** Caesars Forum - Academy 410

### **Description:**

Join the Electronic Frontier Foundation - The leading non-profit fighting for civil liberties in the digital world- to chat about the latest developments in Tech and Law and how these can help each other to build a better future.

The discussion will include updates on current EFF issues such as Disciplinary technologies, Stalkerware, LGBTQ+ Rights, Reproductive Rights, drones, updates on cases and legislation affecting security research, and law enforcement partnerships with industry.

Half of this session will be given over to question-and-answer, so it's your chance to ask EFF questions about the law and tech.

---

[Return to Index](#) - Add to



- ics [Calendar](#) file

---

## **PLV - Friday - 19:00-19:59 PDT**

---

**Title:** Meet the Feds: CISA Edition (Lounge)

**When:** Friday, Aug 12, 19:00 - 19:59 PDT

**Where:** Caesars Forum - Summit 226-227 - Policy Roundtable

**SpeakerBio:**CISA Staff

No BIO available

### **Description:**

Following the fireside chat with US Cybersecurity and Infrastructure Security Agency (CISA) Director, Jen Easterly, several members of the CISA team will be on hand to provide a more in depth look at the Agency, their work, and some of the ways they're already engaging with the hacker community. This session will give hackers an opportunity to ask questions of the CISA team and provide candid feedback to them.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## **PLV - Friday - 20:00-21:59 PDT**

---

**Title:** Meet the Feds: DHS Edition (Lounge)

**When:** Friday, Aug 12, 20:00 - 21:59 PDT

**Where:** Caesars Forum - Summit 226-227 - Policy Roundtable

**SpeakerBio:**DHS Staff

No BIO available

### **Description:**

Members several DHS departments will be on hand to discuss issues they address daily, as well as meet the DEF CON community. Representatives from across DHS are expected, including the Secret Service, Coast Guard, Transportaiton Safety Administration, and the Office of the Secretary.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## **BHV - Sunday - 10:30-11:59 PDT**

---

**Title:** Memento Vivere: A connected light installation on cerebral (dys)function

**When:** Sunday, Aug 14, 10:30 - 11:59 PDT

**Where:** Flamingo - Laughlin I,II,III

**SpeakerBio:**Rick Martinez Herrera

"Ricardo Martinez Herrera (Riikc) is a Mexican artist based in Brussels, Belgium. His work focuses on the intersections of technology and art, including themes related to human anatomy; mathematics, particularly geometric patterns found in nature; and the interactions between nature and the built environment. His artistic approach focuses on combining traditional methods with new materials and approaches, to highlight the continued or even renewed relevance of ancient techniques.

A self-taught approach underlies much of his artistic work. To fund his studies in sculpture, Riikc spent 10 years working in the digital sector, as a web developer and visual content creator. After finishing his MFA in sculpture (2016) at the Académie Royale des Beaux Arts in Brussels, Ricardo then launched his own technology and communications agency. Today, Riikc draws on his experiences in both the fine arts and the technology sectors, to create artwork that spans several genres, including metalwork; digital art; 3D printing and drawing; connected art; and mixed media artwork.

Since 2017, Ricardo has been working with the 3D pen company, 3Doodler, to develop their STEAM education strategy and content. His approach has focused on how this new, hands-on technology can be used to make science education — in particular human, animal, and plant anatomy — more accessible.

In 2021, Ricardo received a research grant from the Fédération Wallonie-Bruxelles to continue his sculptural work. This grant supports his materials research into 3D pen and bronze sculpting, as well as the development of a connected light installation using IoT capture points."

## Description:

"This light installation ""Memento Vivere"" is made up of several connected objects, which will interact with spectators as they pass through the event space. The aim of this multidisciplinary project is to give viewers an experience at the intersection of art and technology, by pushing the public to think critically about the relationship between technology and cognitive function (or even dysfunction).

The installation consists of a series of electroluminescent cables that emerge out of a skull structure built using 3D pen technology. The cables together form a massive connected object, which responds to the interactions of its spectators. Different cables and sectors of the installation will light up according to the movement in front of the piece, the acoustic vibration, and the electronic objects that are present in the room. The spectator is thus encouraged to move and walk in front of the installation, to discover the actions that stimulate the brain.

The IoT technology used in this piece reflects the guiding question of this project: over time, how does the Internet influence our mental functions, human creativity, and the connections between people? IoT sensors can be used to stimulate, and perhaps even expand, the brain's function. However, when taken to its extreme, the overstimulation generated by a constant flow of information from IoT capture points to the brain, leads to a degradation of some of the functions that make up the foundation of a human being. I hope to convey the message that technology creates an important bridge between people and ideas, while encouraging healthy criticism or interrogation of the influence that digital tools have in our lives.

This project is being developed in collaboration with Dr. Frederik Van Gestel, a neuroscience researcher at UZ Brussel, who focuses on the uses of XR technologies in neuro rehabilitation. This piece was first initiated through research funding provided by the Fédération Wallonie-Bruxelles."

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## DL - Saturday - 10:00-11:55 PDT

---

**Title:** Memfini - A systemwide memory monitor interface for linux

**When:** Saturday, Aug 13, 10:00 - 11:55 PDT

**Where:** Caesars Forum - Caucus Boardroom

**Speakers:** Shubham Dubey, Rishal Dwivedi

### Speaker Bio: Shubham Dubey

Shubham is a Security Researcher 2 at Microsoft where he works for Microsoft's defender product. His expertise lies in low level security and internals which includes reverse engineering, exploitation and firmware security. Prior to joining Microsoft, Shubham was Security researcher at Antivirus company working in exploit prevention team where he contributed to protect

customers from 0days and vulnerabilities in the wild. Shubham has worked on multiple independent project on kernel level and firmware security. He own a security blog nixhacker.com where you will find lots of content on low level security and internals.

### **SpeakerBio:**Rishal Dwivedi

Rishal is a Security Researcher at Microsoft where he works for Microsoft's defender product. His expertise lies in Offensive security which includes vulnerability discovery and exploitation, owning multiple CVE's. Prior to joining Microsoft, Rishal was a Sr. Security researcher at company where he contributed to their Web Application Security product. Rishal gained fame in bug bounty at an early age of 13 years. After contributing to Application Security for multiple years, he went on to explore other domains of security including IOT security and Malware Analysis.

### **Description:**

Surprisingly, memory related events logging has been ignored by monitoring tool's authors since a long time. There are multiple event loggers present for Linux that are capable of monitoring processes, i/o operations, function calls or whole systemwide events. But something which lacks in most is global monitoring of memory related events like allocation, attachment to a shared memory, memory allocation in foreign process etc. This has many applications in security domain or even software engineering in general. The main area of focus or use case for Memfini is to assist Security professionals for carrying out memory specific Dynamic Malware Analysis, in order to help them in finding indicators for malicious activities without reversing the behavior. Below listed are few of the use cases (which we will also be demonstrating in the talk). • Process Injection • Fileless malware execution • Shellcode Execution • Malicious shared memory usage On the other hand, it can also be helpful for Software developers, who wish to have an eagle eye on the memory allocations • Finding Memory Leaks • Error detection for debugging purposes. The is possible as Memfini is capable of monitoring memory allocations on User space, Kernel space as well as some under looked allocations like PCI device mapping, DMA allocations etc. It provides a command line interface with multiple filters, allowing a user to interact with the logs generated & get the required data. Currently, the user will be able to filter the events by individual process, type of access etc.

Audience: Defensive security(Malware researcher, IR/Forensics) and Offensive security(memory based vulnerability discovery)

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

### **DC - Sunday - 09:00-14:59 PDT**

---

**Title:** Merch (formerly swag) Area Open -- README

**When:** Sunday, Aug 14, 09:00 - 14:59 PDT

**Where:** Caesars Forum - Summit 229

### **Description:**

The published hours for the merch area are only an approximation: supplies are limited, and when merch is sold out, the merch area will close. (We intend to update this schedule to reflect their true operating status, but this is strictly best-effort.)

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

### **DC - Friday - 09:00-15:59 PDT**

---

**Title:** Merch (formerly swag) Area Open -- README

**When:** Friday, Aug 12, 09:00 - 15:59 PDT

**Where:** Caesars Forum - Summit 229

## Description:

The published hours for the merch area are only an approximation: supplies are limited, and when merch is sold out, the merch area will close. (We intend to update this schedule to reflect their true operating status, but this is strictly best-effort.)

---

[Return to Index](#) - Add to



- ics [Calendar](#) file

---

## DC - Saturday - 09:00-15:59 PDT

---

**Title:** Merch (formerly swag) Area Open -- README

**When:** Saturday, Aug 13, 09:00 - 15:59 PDT

**Where:** Caesars Forum - Summit 229

## Description:

The published hours for the merch area are only an approximation: supplies are limited, and when merch is sold out, the merch area will close. (We intend to update this schedule to reflect their true operating status, but this is strictly best-effort.)

---

[Return to Index](#) - Add to



- ics [Calendar](#) file

---

## DL - Friday - 12:00-13:55 PDT

---

**Title:** Mercury

**When:** Friday, Aug 12, 12:00 - 13:55 PDT

**Where:** Caesars Forum - Society Boardroom

**Speakers:**David McGrew,Brandon Enright

### **SpeakerBio:**David McGrew

David McGrew leads research and development into the detection of threats, vulnerabilities, and attacks using network data. He designed authenticated encryption algorithms and protocols, most notably GCM and Secure RTP, and he is a Fellow at Cisco Systems.

### **SpeakerBio:**Brandon Enright

Brandon Enright is a lead DIFR investigator for Cisco CSIRT, an expert at DNS and network data analysis, and a contributor to Nmap and other open source projects.

## Description:

Mercury is an open source package for network metadata extraction and analysis. It reports session metadata including fingerprint strings for TLS, QUIC, HTTP, DNS, and many other protocols. Mercury can output JSON or PCAP. Designed for large scale use, it can process packets in real time at 40Gbps on server-class commodity hardware, using Linux native zero-copy high performance networking. The Mercury package includes tools for analyzing PKIX/X.509 certificates and finding weak keys, and for analyzing fingerprints with destination context using a naive Bayes classifier.

Audience: Network defense, incident response, forensics, security and privacy research

---

[Return to Index](#) - Add to



- ics [Calendar](#) file

---

**Title:** Metal and Fire... Copying Keys via Mold and Cast Tactics

**When:** Saturday, Aug 13, 11:00 - 11:30 PDT

**Where:** Caesars Forum - Summit 203-204, 235

**SpeakerBio:** Deviant Ollam

No BIO available

### Description:

You've seen lockpickers open doors by manipulating pins. Such a tactic relies on ownership of pick tools and the knowledge of how to use them.

You may have witnessed hackers demonstrate the art of impressioning. Such a technique requires a working blank key that can be hand-filed into the correct shape in order to facilitate entry.

But have you ever seen a key fabricated before your eyes from nothing at all? With a raw ingot of metal ore, heat from a flame, and some subversive skill it's possible to re-create almost any key -- no matter how obscure -- via molding and casting. That is what this presentation entails: keys will be created using raw metal and fire. But not in a forge or foundry... this is a tactic that can be employed in the field by covert entry types who want a way to gain repeated access without having to carry around key blanks and specific tools specialized for every brand of lock.

When you're casting a key from nothing, virtually any kind of mechanical lock becomes a valid target.

---

[Return to Index](#) - Add to



- ics [Calendar](#) file

---

## RHV - Friday - 15:00-15:59 PDT

---

**Title:** Mitigating vulnerabilities in two-factor authentication in preventing account takeover

**When:** Friday, Aug 12, 15:00 - 15:59 PDT

**Where:** Caesars Forum - Alliance 310, 320

**SpeakerBio:** Larsbodian

Larsbodian is an industrial PhD student at the Department of Computer and Systems Sciences at Stockholm University in Sweden researching IoT security integration within Enterprise Architecture.

### Description:

Working in banking, merchant services providers such as Klarna, and conducting forensic investigations, there are some important considerations about how to implement 2FA that is resilient to the human factor. Larsbodian will discuss actual experiences in fraud and account takeover and how vulnerabilities in how 2FA works when combined with humans can be mitigated.

---

[Return to Index](#) - Add to



- ics [Calendar](#) file

---

## SOC - Friday - 20:00-23:59 PDT

---

**Title:** Movie Night Double Feature - Arrival & Real Genius

**When:** Friday, Aug 12, 20:00 - 23:59 PDT

**Where:** Caesars Forum - Academy 401-410, 421 (Track 3)

### Description:

Chills! Thrills! A quiet place to sit down! 2 Movies for the price of none!

Arrival - A linguist works with the military to communicate with alien lifeforms after mysterious spacecraft appear around the world.

Real Genius - Yet another in a long series of diversions in an attempt to avoid responsibility.

---

[Return to Index](#) - Add to

[Google Calendar](#)

- ics [Calendar](#) file

---

## SOC - Saturday - 20:00-23:59 PDT

---

**Title:** Movie Night Double Feature - The Conversation & The 13th Floor

**When:** Saturday, Aug 13, 20:00 - 23:59 PDT

**Where:** Caesars Forum - Academy 401-410, 421 (Track 3)

### Description:

Chills! Thrills! A quiet place to sit down! 2 Movies for the price of none!

The Conversation - A paranoid, secretive surveillance expert has a crisis of conscience when he suspects that the couple he is spying on will be murdered.

The 13th Floor - A computer scientist a virtual reality simulation of 1937 becomes the primary suspect when his colleague and mentor is murdered.

---

[Return to Index](#) - Add to

[Google Calendar](#)

- ics [Calendar](#) file

---

## HHV - Friday - 14:00-14:45 PDT

---

**Title:** Movie-Style Hardware Hacking

**When:** Friday, Aug 12, 14:00 - 14:45 PDT

**Where:** Flamingo - Exec Conf Ctr - Red Rock VI, VII, VII

### SpeakerBio:

Bryan C. Geraghty

Bryan leads and executes highly technical software and hardware assessments. He specializes in cryptography, reverse engineering, and analyzing complex threat models.

### Description:

We all have hardware devices sitting around: In server rooms or your IoT devices at home. What are these things actually doing? It would be really handy to have root access on them to aid us in future adventures.

Or maybe you want to perma-root the device and re-sell it to some unsuspecting victim. Or maybe you want to know if you're the unsuspecting victim. Who am I to judge?

What does it take to cause these devices to fail? Can we get them to fail open?

I'm going to tell a story about circuit-shorting attacks, how to build a hardware circuit to perform this attack with a computer, and give you the instructions and code to build one yourself... with a device you may already have :)

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## PLV - Friday - 16:00-17:45 PDT

---

**Title:** Moving Regulation Upstream - An Increasing focus on the Role of Digital Service Providers

**When:** Friday, Aug 12, 16:00 - 17:45 PDT

**Where:** Caesars Forum - Summit 226-227 - Policy Roundtable

**Speakers:**Jen Ellis,Irfan Hemani,Adam Dobell

**SpeakerBio:**Jen Ellis , Vice President of Community and Public Affairs

No BIO available

**SpeakerBio:**Irfan Hemani , Deputy Director - Cyber Security, Cyber Security and Digital Identity Directorate, UK

Department for Digital, Culture, Media and Sport

No BIO available

**SpeakerBio:**Adam Dobell , First Secretary, Department of Home Affairs, Embassy of Australia

No BIO available

### Description:

Cybercriminals are no longer focusing all their efforts on the biggest fish, which means organizations below the security poverty line - who often struggle with achieving adequate cyber resilience - are increasingly being hit. At the same time, we've seen an increase in supply chain attacks, which makes sense as more and more of the tech ecosystem is moving to cloud or managed service provider models. Various governments are paying attention to these shifts and are considering how regulating digital service providers may advance security more broadly, while also alleviating the burden on small to medium businesses. This session will be led by one or two governments working on this issue and will include an open discussion on the challenges and opportunities of this approach.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## MIV - Friday - 14:30-15:59 PDT

---

**Title:** Multi-Stakeholder Online Harm Threat Analysis

**When:** Friday, Aug 12, 14:30 - 15:59 PDT

**Where:** Caesars Forum - Summit 221->236

**SpeakerBio:**Jennifer Mathieu

Jennifer Mathieu, PhD, is Chief Technology Officer at Graphika. She brings extensive experience building robust, integrated, cloud-based solutions to the company, enabling customers to tackle the threat of disinformation. Jennifer is responsible for guiding the company's technology vision, continuing the evolution of Graphika's patented technology, strengthening its core products, and building out the company's team of expert engineers and architects.

## Description:

No Description available

---

[Return to Index](#) - Add to



- ics [Calendar](#) file

---

## DC - Saturday - 11:00-11:45 PDT

---

**Title:** My First Hack Was in 1958 (Then A Career in Rock'n'Roll Taught Me About Security)

**When:** Saturday, Aug 13, 11:00 - 11:45 PDT

**Where:** Caesars Forum - Forum 106-110, 138-139 (Track 2)

**SpeakerBio:** Winn Schwartau , Security Thinker Since 1983

“After talking to Winn for an hour and a half, you’re like, what the f\*\*\* just happened? - Bob Todrank

Winn has lived Cybersecurity since 1983, and now says, “I think, maybe, I’m starting to understand it.” Since 1988, his predictions about security have been scarily spot on. He coined “Electronic Pearl Harbor” while testifying before Congress in 1991 and prognosticated a future with massive surveillance, loss of personal privacy, nation-state hacking, cyberwar and cyber-terrorism. He was named the “Civilian Architect of Information Warfare,” by Admiral Tyrrell of the British MoD.

His latest book, “Analogue Network Security” is a math and time-based, probabilistic approach to security with designs “fix security and the internet. It will twist your mind.

Fellow, Royal Society of the Arts

Distinguished Fellow: Ponemon Institute Int'l Security Hall of Fame: ISSA

Top 20 industry pioneers: SC Magazine

Top 25 Most Influential: Security Magazine Top 5 Security Thinkers: SC Magazine

Power Thinker (and one of 50 most powerful people) Network World Top Rated (4.85/5) RSA Speaker

Top Rated ISC2: 4.56

.001% Top Influencer RSAC 2019

Author: Information Warfare, CyberShock, Internet & Computer Ethics for Kids, Time Based Security, Pearl Harbor Dot Com  
(Die Hard IV) Founder: [www.TheSecurityAwarenessCompany.Com](http://www.TheSecurityAwarenessCompany.Com) Producer: Hackers Are People Too

Twitter: [@https://twitter.com/WinnSchwartau](https://twitter.com/WinnSchwartau)

## Description:

My first hack was in 1958, and it was all my mother’s fault. Or perhaps I should also blame my father. They were both engineers and I got their DNA. As a kid I hacked phones... cuz, well, phones were expensive! (Cardboard was an important hacking tool.) At age 6 I made a decent living cuz I could fix tube TVs. True!

In roughly 1970 (thanks to NYU) we moved on to hacking Hollerith (punch) cards to avoid paying for telephone and our utilities, and of course, shenanigans.

As a recording studio designer and builder, we dumpster dived for technology from AT&T. We never threw anything out and learned how to repurpose and abuse tech from the 1940s.

As a rock’n’roll engineer, I learned to live with constant systems epic failures. Anything that could break would break: before a live TV event or a massive concert. Talk about lessons in Disaster Recovery and Incident Response.

This talk, chock full of pictures and stories from the past, covers my hacking path as a kid then as a necessary part of survival in the entertainment industry. 1958-1981.

Come on down for the ride and see how 64 years of lessons learned can give you an entirely different view of Hacking and how and why I have embraced failure for both of my careers!

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## BHV - Saturday - 10:00-10:30 PDT

---

**Title:** NASA + Healthcare ...

**When:** Saturday, Aug 13, 10:00 - 10:30 PDT

**Where:** Flamingo - Laughlin I,II,III

**SpeakerBio:**Dr. Josef Schmid

No BIO available

**Description:**No Description available

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## BHV - Saturday - 14:30-14:59 PDT

---

**Title:** Natural Disasters and International Supply Chains: Biomedical and Pharmaceutical Review

**When:** Saturday, Aug 13, 14:30 - 14:59 PDT

**Where:** Flamingo - Laughlin I,II,III

**SpeakerBio:**Jorge Acevedo Canabal , MD

No BIO available

**Description:**No Description available

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## ASV - Saturday - 15:00-15:50 PDT

---

**Title:** Near and Far: Securing On and Off Planet Networks at JPL

**When:** Saturday, Aug 13, 15:00 - 15:50 PDT

**Where:** Caesars Forum - Forum 112-117

**SpeakerBio:**Wes Gavins

As CISO, Wes provides strategic direction for all IT security technology areas including applications, networks and storage; serves as the authority and primary JPL representative on internal and external security architecture teams; selects solutions to enhance security controls; and conduct risk assessments for major Lab-wide processes and make major security risk decisions.

**Description:**

If you know the names Voyager 1 and 2, Galileo, Salvage 1, Hubble, Cassini, Opportunity, and Spirit then you are familiar with the work done by NASA's Jet Propulsion Laboratory. But space operations are more than just the satellites and vehicles we typically hear about, and JPL's Chief Information Security Officer is responsible for keeping the variety of complex ground networks continuously running. Join us to hear from Wes Gavins, CISO at JPL, and learn about his infosec journey, his inspiration, and how he leads his teams to ensure safe and secure space operations.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## WS - Thursday - 10:00-13:59 PDT

---

**Title:** Network Hacking 101

**When:** Thursday, Aug 11, 10:00 - 13:59 PDT

**Where:** Harrah's - Ely

**Speakers:** Victor Graf, Ben Kurtz

**SpeakerBio:** Victor Graf , Hacker

Victor is a hacker and software engineer from Seattle with a love of network security and cryptography. He most recently worked for a blockchain company designing and building peer-to-peer protocols and systems for non-custodial account recovery. Building and breaking networks was his first love in the world of computers, and he built the Naumachia platform starting in 2017 to bring network hacking to CTFs. With that he has hosted Network Hacking 101 workshops in San Francisco and now in Seattle.

**SpeakerBio:** Ben Kurtz , Hacker

Ben Kurtz is a hacker, a hardware enthusiast, and the host of the Hack the Planet podcast ([symbolcrash.com/podcast](http://symbolcrash.com/podcast)). After his first talk, at DefCon 13, he ditched development and started a long career in security.

He has been a pentester for IOActive, head of security for an MMO company, and on the internal pentest team for the Xbox One at Microsoft. Along the way, he volunteered on anti-censorship projects, which resulted in his conversion to Golang and the development of the ratnet project ([github.com/awgh/ratnet](https://github.com/awgh/ratnet)). A few years ago, he co-founded the Binject group to develop core offensive components for Golang-based malware, and Symbol Crash, which focuses on sharing hacker knowledge through trainings for red teams, a free monthly Hardware Hacking workshop in Seattle, and podcasts. He is currently developing a ratnet-based handheld device for mobile encrypted mesh messaging ([www.crowdsupply.com/improv-labs/meshinger](http://www.crowdsupply.com/improv-labs/meshinger)).

### Description:

Come learn how to hack networks without needing to piss off your local coffee shop, housemates, or the Feds! Bring your laptop and by the end of this workshop, everyone can walk away having intercepted some packets and popped some reverse shells.

In the workshop you'll solve a series of challenges, each in a contained virtualized network where it's just you and your targets. We'll start with a networking crash course to introduce you to packets and their layers, as well as how to use Wireshark to dig in and explore further. We'll practice network sniffing and scanning to find your targets, and of course how to execute a man-in-the-middle attack via ARP spoofing to intercept local network traffic. With those techniques, we'll go through challenges including extracting plaintext passwords, TCP session hijacking, DNS poisoning, and SMTP TLS downgrade. All together, this workshop aims to give you the tools you need to start attacking systems at the network layer.

### Materials

A laptop with Linux or a Linux VM (MacOS can also work, but have a VM installed as a backup). These software tools (detailed installation instructions will be provided in the materials ahead of DEFCON):

- ◊ OpenVPN: Connect to the challenges you will be hacking

- ◊ Wireshark (tcpdump also works): Capture and dissect network traffic
- ◊ netcat (nc): Swiss-army-knife of networking
- ◊ nmap: Scan and search for vulnerable targets
- ◊ bettercap: Man-in-the-middle attack tool and network attack platform
- ◊ python3 (optional): Build new attack tools

Prereq

Basic experience with Linux command-line tools

Basic familiarity with networking (e.g. you know what IP and MAC addresses are, you could set up your home router, and host a LAN party)

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## BICV - Saturday - 16:00-16:30 PDT

---

**Title:** Neurodiversity in Cybersecurity: Find Your Competitive Advantage!

**When:** Saturday, Aug 13, 16:00 - 16:30 PDT

**Where:** Virtual - BIC Village

**Speakers:**Kassandra Pierre,Nathan Chung

**SpeakerBio:**Kassandra Pierre

No BIO available

**SpeakerBio:**Nathan Chung

No BIO available

**Description:**No Description available

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## SOC - Saturday - 18:00-01:59 PDT

---

**Title:** Night of the Ninjas - Entertainment

**When:** Saturday, Aug 13, 18:00 - 01:59 PDT

**Where:** Caesars Forum - Forum 120-123, 129, 137

**Speakers:**Scotch and Bubbles,TAIKOPROJECT,Z3NPI,Zebbler Encanti Experience,CTRL/rsm,Krisz Klink,Magician Kody Hildebrand,Mass Accelerator

**SpeakerBio:**Scotch and Bubbles

No BIO available

**SpeakerBio:**TAIKOPROJECT

No BIO available

**SpeakerBio:**Z3NPI

No BIO available

**SpeakerBio:**Zebbler Encanti Experience

No BIO available

**SpeakerBio:**CTRL/rsm

No BIO available

**SpeakerBio:**Krisz Klink

No BIO available

**SpeakerBio:**Magician Kody Hildebrand

No BIO available

**SpeakerBio:**Mass Accelerator

No BIO available

### Description:

18:00 - 19:00: Hildebrand Magic

19:00 - 20:00: Scotch and Bubbles

20:00 - 21:00: Z3npi

21:00 - 22:00: Mass Accelerator

22:00 - 23:00: Krisz Klink

**23:00 - 00:00: TAIKOPROJECT**

00:00 - 00:15: Costume Contest

00:15 - 01:00: Zebbler Encanti Experience 01:00 - 02:00: CTRL/rsm

[Return to Index](#) - Add to

[Google Calendar](#)

- ics [Calendar](#) file

## DDV - Friday - 15:00-15:59 PDT

**Title:** No bricks without clay - Data Fusion and Duplication in Cybersecurity

**When:** Friday, Aug 12, 15:00 - 15:59 PDT

**Where:** Flamingo - Exec Conf Ctr - Lake Meade and Valley of Fire

**SpeakerBio:**Lior Kolnik

Lior Kolnik is a Security Research Leader with a passion for defending organizations and solving complex problems. During his 13 years in cybersecurity Lior has collaborated with security teams at Fortune 50 companies, completed a 7-year service in an elite tech unit of the Israeli IDF and earned his M.Sc. in CyberSecurity.

### Description:

"How do Cybersecurity professionals decide if they are looking at a false alarm or a breach in progress? The answer is data. Securing an organization is all about data - collecting, storing, analyzing. Where is all this data coming from? How is it being used and when? What are the causes of data duplication throughout this practice and when is it necessary? In this talk we will discuss these subjects in detail, review different models and their strengths and weaknesses."

[Return to Index](#) - Add to

[Google Calendar](#)

- ics [Calendar](#) file

## DC - Saturday - 11:00-11:45 PDT

---

**Title:** No-Code Malware: Windows 11 At Your Service

**When:** Saturday, Aug 13, 11:00 - 11:45 PDT

**Where:** Caesars Forum - Academy 401-410, 421 (Track 3)

**SpeakerBio:** Michael Bargury , Co-Founder and CTO, Zenity.io

Michael Bargury is the Co-Founder and CTO of Zenity, where he helps companies secure their low-code/no-code apps. In the past, he headed security product efforts at Azure focused on IoT, APIs and IaC. Michael is passionate about all things related to cloud, SaaS and low-code security, and spends his time finding ways they could go wrong. He also leads the OWASP low-code security project and writes about it on DarkReading.

Twitter: [@https://twitter.com/mbrg0](https://twitter.com/mbrg0)

### Description:

Windows 11 ships with a nifty feature called Power Automate, which lets users automate mundane processes. In a nutshell, Users can build custom processes and hand them to Microsoft, which in turn ensures they are distributed to all user machines or Office cloud, executed successfully and reports back to the cloud. You can probably already see where this is going.. In this presentation, we will show how Power Automate can be repurposed to power malware operations. We will demonstrate the full cycle of distributing payloads, bypassing perimeter controls, executing them on victim machines and exfiltrating data. All while using nothing but Windows baked-in and signed executables, and Office cloud services. We will then take you behind the scenes and explore how this service works, what attack surface it exposes on the machine and in the cloud, and how it is enabled by-default and can be used without explicit user consent. We will also point out a few promising future research directions for the community to pursue. Finally, we will share an open-source command line tool to easily accomplish all of the above, so you will be able to add it into your Red Team arsenal and try out your own ideas.

---

[Return to Index](#) - Add to



- ics [Calendar](#) file

---

## MIV - Saturday - 16:15-16:45 PDT

---

**Title:** Not Feeling Yourself: User Spoofing and Other Disinformation Exploits

**When:** Saturday, Aug 13, 16:15 - 16:45 PDT

**Where:** Caesars Forum - Summit 221->236

**SpeakerBio:** Erica Burgess

Burninator was a software engineer, bot developer and hobbyist hacker before becoming an appsec redteamer in 2018, and has been hacking all the things since high school.

**Description:**No Description available

---

[Return to Index](#) - Add to



- ics [Calendar](#) file

---

## CLV - Saturday - 10:00-10:40 PDT

---

**Title:** OAuth-some Security Tricks: Yet more OAuth abuse

**When:** Saturday, Aug 13, 10:00 - 10:40 PDT

**Where:** Flamingo - Scenic Ballroom

## **SpeakerBio:**Jenko Hwong

Jenko Hwong is a Principal Researcher on Netskope's Threat Research Team, focusing on cloud threats/vectors. He's spent time in engineering and product roles at various security startups in vulnerability scanning, AV/AS, pen-testing/exploits, L3/4 appliances, threat intel, and windows security.

Twitter: [@https://twitter.com/jenkohwong](https://twitter.com/jenkohwong)

## **Description:**

Join in this deep dive looking at new abuses of OAuth 2.0. We'll look at a variety of attacks including phishing and stolen credential attacks, starting with Microsoft authorization code grant to Google authorization code grant using copy/paste. We'll then move on to new attacks including: OWA browser attacks, Chrome attacks, different SaaS OAuth implementations, upstream SSO attacks, and hidden uses of OAuth in Google App Scripting and Google Cloud Shell.

In a nod to Penn and Teller, with each attack, we'll reveal the underlying secret techniques used, why and how it works, and what can be generalized. We'll then show how the most common defensive measures (e.g. MFA, IP allow lists, application allow lists, authorization controls) are used to mitigate each attack, then adjust the attack to bypass the defensive measure. We'll also discuss what vendors have been doing to mitigate these attacks and whether they are effective.

Code for any demo/POCs will be made available as open-source.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## **BTV - Friday - 14:00-14:59 PDT**

---

**Title:** Obsidian CTH Live: Killchain 1 Walkthrough

**When:** Friday, Aug 12, 14:00 - 14:59 PDT

**Where:** Flamingo - Savoy Ballroom - BTV Main Stage

## **Description:**

Come take a dive into the data lake and cast some queries to find proof that users have run files from malicious actors. How can we prove the existence of troublesome activity in the environment?

Blue Team Village's Project Obsidian is an immersive, defensive cybersecurity learning experience that provides attendees with the opportunity to gain knowledge of Incident Response (IR), Digital Forensics (DF), Reverse Engineering Malware (REM), Cyber Threat Intelligence (CTI), and Cyber Threat Hunting (CTH).

Come take a dive into the data lake and cast some queries to find proof that users have run files from malicious actors. How can we prove the existence of troublesome activity in the environment?

Blue Team Village's Project Obsidian is an immersive, defensive cybersecurity learning experience that provides attendees with the opportunity to gain knowledge of Incident Response (IR), Digital Forensics (DF), Reverse Engineering Malware (REM), Cyber Threat Intelligence (CTI), and Cyber Threat Hunting (CTH).

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## **BTV - Saturday - 13:00-13:59 PDT**

---

**Title:** Obsidian CTH Live: Killchain 3 Walkthrough

**When:** Saturday, Aug 13, 13:00 - 13:59 PDT

**Where:** Flamingo - Savoy Ballroom - BTV Main Stage

## Description:

Obsidian CTH Live: Killchain 3 Walkthrough

Blue Team Village's Project Obsidian is an immersive, defensive cybersecurity learning experience that provides attendees with the opportunity to gain knowledge of Incident Response (IR), Digital Forensics (DF), Reverse Engineering Malware (REM), Cyber Threat Intelligence (CTI), and Cyber Threat Hunting (CTH).

Obsidian CTH Live: Killchain 3 Walkthrough

Blue Team Village's Project Obsidian is an immersive, defensive cybersecurity learning experience that provides attendees with the opportunity to gain knowledge of Incident Response (IR), Digital Forensics (DF), Reverse Engineering Malware (REM), Cyber Threat Intelligence (CTI), and Cyber Threat Hunting (CTH).

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## BTV - Friday - 10:30-11:30 PDT

---

**Title:** Obsidian CTH: Go Phish: Visualizing Basic Malice

**When:** Friday, Aug 12, 10:30 - 11:30 PDT

**Where:** Flamingo - Savoy Ballroom - BTV Project Obsidian: Track 0x42

**SpeakerBio:** SamunoskeX

No BIO available

## Description:

Come take a dive into the data lake and cast some queries to find proof that users have run files from malicious actors. How can we prove the existence of troublesome activity in the environment? We will take a journey as if we are a new member of the Magnum Tempus Financial Security Team and proceed through a Threat Hunt through the eyes of a newbie in the field of Threat Hunting.

Blue Team Village's Project Obsidian is an immersive, defensive cybersecurity learning experience that provides attendees with the opportunity to gain knowledge of Incident Response (IR), Digital Forensics (DF), Reverse Engineering Malware (REM), Cyber Threat Intelligence (CTI), and Cyber Threat Hunting (CTH).

Come take a dive into the data lake and cast some queries to find proof that users have run files from malicious actors. How can we prove the existence of troublesome activity in the environment? We will take a journey as if we are a new member of the Magnum Tempus Financial Security Team and proceed through a Threat Hunt through the eyes of a newbie in the field of Threat Hunting.

Blue Team Village's Project Obsidian is an immersive, defensive cybersecurity learning experience.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## BTV - Friday - 13:00-13:59 PDT

---

**Title:** Obsidian CTH: Hunting for Adversary's Schedule

**When:** Friday, Aug 12, 13:00 - 13:59 PDT

**Where:** Flamingo - Savoy Ballroom - BTV Project Obsidian: Track 0x42

**SpeakerBio:**Cyb3rHawk

No BIO available

### Description:

Once an adversary gained a foothold, they typically would like to keep their access. Here, I'm using the term ""access"" loosely where it could be many things like C2 beacon, script, binary, security source providers, shortcuts, and so on. This is called Persistence and in MITRE speak ""TA0003"" [3]. We take a look at one such persistence method, Scheduled Task. Scheduled tasks are one of the most commonly used persistence techniques in adversary intrusions and for a good reason. It provides flexibility to be created on local and remote machines and provides several ways to be created (from GUI to Net32API), along with the ability to combine/achieve tactics like Execution and Privilege Escalation. We start with the basics of scheduled tasks, and why and when an adversary would like to use them. Then we jump into the hell of threat hunting to see some ways to create a hypothesis and investigate the result set. In the end, we take a stab at detection engineering concepts surrounding the creation/revision of detections/analytics from queries/results we got from hunting this technique.

Blue Team Village's Project Obsidian is an immersive, defensive cybersecurity learning experience that provides attendees with the opportunity to gain knowledge of Incident Response (IR), Digital Forensics (DF), Reverse Engineering Malware (REM), Cyber Threat Intelligence (CTI), and Cyber Threat Hunting (CTH).

Once an adversary gained a foothold, they typically would like to keep their access and establish persistence. Scheduled tasks are one of the most commonly used persistence techniques in adversary intrusions and for a good reason. In this session we take a look at Scheduled Tasks. We start with the basics, and then learn how to create a hypothesis to conduct a threat hunt. In the end, we'll take a stab at detection engineering concepts surrounding the creation/revision of detections/analytics from telemetry we obtain from hunting this technique.

Project Obsidian is an immersive, defensive cybersecurity learning experience.

---

[Return to Index](#) - Add to [!\[\]\(e78c5469bcf77023318e230d5e4d9471\_img.jpg\) Google Calendar](#) - ics [Calendar](#) file

---

## BTV - Saturday - 10:30-11:30 PDT

---

**Title:** Obsidian CTH: Sniffing Compromise: Hunting for Bloodhound

**When:** Saturday, Aug 13, 10:30 - 11:30 PDT

**Where:** Flamingo - Savoy Ballroom - BTV Project Obsidian: Track 0x42

**SpeakerBio:**CerealKiller

No BIO available

### Description:

Join us on a journey as we chase BloodHound through a compromised environment via host and network telemetry. We will dive quickly into detections to become better prepared for next time.

Blue Team Village's Project Obsidian is an immersive, defensive cybersecurity learning experience that provides attendees with the opportunity to gain knowledge of Incident Response (IR), Digital Forensics (DF), Reverse Engineering Malware (REM), Cyber Threat Intelligence (CTI), and Cyber Threat Hunting (CTH).

Join us on a journey as we chase BloodHound through a compromised environment via host and network telemetry. We will dive quickly into detections to become better prepared for next time.

Blue Team Village's Project Obsidian is an immersive, defensive cybersecurity learning experience that provides attendees with the opportunity to gain knowledge of Incident Response (IR), Digital Forensics (DF), Reverse Engineering Malware (REM), Cyber Threat Intelligence (CTI), and Cyber Threat Hunting (CTH).

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## **BTV - Saturday - 14:00-14:59 PDT**

---

**Title:** Obsidian CTH: The Logs are Gone?

**When:** Saturday, Aug 13, 14:00 - 14:59 PDT

**Where:** Flamingo - Savoy Ballroom - BTV Project Obsidian: Track 0x42

**SpeakerBio:**ExtremePaperClip

Digital Forensics Nerd, Linux Geek, InfoSec Dork, Lifelong Student of Everything, Amateur History Buff... Loads of Fun.

### **Description:**

What happens when an attacker clears the logs in an effort to hide their tracks? Here we will dive into that question, build a Threat Hunting hypothesis, develop some ways to detect this activity, and document the process.

Blue Team Village's Project Obsidian is an immersive, defensive cybersecurity learning experience that provides attendees with the opportunity to gain knowledge of Incident Response (IR), Digital Forensics (DF), Reverse Engineering Malware (REM), Cyber Threat Intelligence (CTI), and Cyber Threat Hunting (CTH).

What happens when an attacker clears the logs in an effort to hide their tracks? Here we will dive into that question, build a Threat Hunting hypothesis, develop some ways to detect this activity, and document the process.

Blue Team Village's Project Obsidian is an immersive, defensive cybersecurity learning experience that provides attendees with the opportunity to gain knowledge of Incident Response (IR), Digital Forensics (DF), Reverse Engineering Malware (REM), Cyber Threat Intelligence (CTI), and Cyber Threat Hunting (CTH).

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## **BTV - Friday - 11:30-12:30 PDT**

---

**Title:** Obsidian CTI: Generating Threat Intelligence from an Incident

**When:** Friday, Aug 12, 11:30 - 12:30 PDT

**Where:** Flamingo - Savoy Ballroom - BTV Project Obsidian: Track 0x42

**Speakers:**Stephanie G.,l00sid,ttheveii0x

**SpeakerBio:**Stephanie G.

Stephanie is a security software engineer in the product security space. She is a volunteer on BTV's CTI team for Project Obsidian at DEF CON 30.

**SpeakerBio:**l00sid

l00sid just started a career as a blue teamer. He loves the kinds of puzzles he gets to solve in the process of stopping attackers.

**SpeakerBio:**ttheveii0x

## Description:

This module covers:

- Direction & Planning: Overview of CTI stakeholders and intelligence requirements
- Collection: CTI analysts role during an incident
- Processing: Intrusion data & information
- Analysis & Production: Elements to include in a report
- Dissemination: Sharing the report with stakeholders
- Feedback & Evaluation: Methods for receiving feedback

The objective is to demonstrate the critical role CTI plays both during and after an incident.

Blue Team Village's Project Obsidian is an immersive, defensive cybersecurity learning experience that provides attendees with the opportunity to gain knowledge of Incident Response (IR), Digital Forensics (DF), Reverse Engineering Malware (REM), Cyber Threat Intelligence (CTI), and Cyber Threat Hunting (CTH).

This session presents an overview of how threat intelligence can be generated from an incident and shared with various stakeholders. We'll run through an incident and demonstrate how the CTI team plays a critical role by performing research and providing insights based on stakeholder requirements.

Blue Team Village's Project Obsidian is an immersive, defensive cybersecurity learning experience that provides attendees with the opportunity to gain knowledge of Incident Response (IR), Digital Forensics (DF), Reverse Engineering Malware (REM), Cyber Threat Intelligence (CTI), and Cyber Threat Hunting (CTH).

---

[Return to Index](#) - Add to



- ics [Calendar](#) file

---

## **BTW - Saturday - 11:30-12:30 PDT**

---

**Title:** Obsidian CTI: Operationalizing Threat Intelligence

**When:** Saturday, Aug 13, 11:30 - 12:30 PDT

**Where:** Flamingo - Savoy Ballroom - BTW Project Obsidian: Track 0x42

**Speakers:**Stephanie G.,l00sid,ttheveii0x

**SpeakerBio:**Stephanie G.

Stephanie is a security software engineer in the product security space. She is a volunteer on BTW's CTI team for Project Obsidian at DEF CON 30.

**SpeakerBio:**l00sid

l00sid just started a career as a blue teamer. He loves the kinds of puzzles he gets to solve in the process of stopping attackers.

**SpeakerBio:**ttheveii0x

Mentor, Hacker, Cyber Threat Intelligence, Reverse Engineering Malware, OSINT, 70757a7a6c6573, Blue Team Village Director, Consultant

## Description:

This module covers:

- Direction & Planning: Establishing CTI goals and objectives
- Collection: Objective is to review and operationalize a single CTI report
- Analysis & Production: Elements to identify in a CTI report
- Dissemination: Sharing takeaways from a CTI report with stakeholders
- Feedback & Evaluation: Methods for receiving feedback

Objective: Demonstrate how a CTI report can be operationalized.

Blue Team Village's Project Obsidian is an immersive, defensive cybersecurity learning experience that provides attendees with the opportunity to gain knowledge of Incident Response (IR), Digital Forensics (DF), Reverse Engineering Malware (REM), Cyber Threat Intelligence (CTI), and Cyber Threat Hunting (CTH).

This module presents an overview of how threat intelligence gleaned from a single CTI report can be operationalized across an organization. We'll run through a report based on content from Project Obsidian's kill chain 3 and demonstrate how it can be operationalized by different teams (SOC, IR, forensics, security management, and executives).

Blue Team Village's Project Obsidian is an immersive, defensive cybersecurity learning experience that provides attendees with the opportunity to gain knowledge of Incident Response (IR), Digital Forensics (DF), Reverse Engineering Malware (REM), Cyber Threat Intelligence (CTI), and Cyber Threat Hunting (CTH).

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## **BTV - Saturday - 14:30-14:59 PDT**

---

**Title:** Obsidian Forensics: Creating a custom Velociraptor collector

**When:** Saturday, Aug 13, 14:30 - 14:59 PDT

**Where:** Flamingo - Savoy Ballroom - BTV Project Obsidian: Track 0x41

**Speakers:**Wes Lambert,Omenscan

**SpeakerBio:**Wes Lambert

No BIO available

**SpeakerBio:**Omenscan

Obsidian Forensics Lead

### **Description:**

Obsidian 4n6 Station: Pre-Recorded - Obsidian 4n6: Creating a custom Velociraptor collector

Blue Team Village's Project Obsidian is an immersive, defensive cybersecurity learning experience that provides attendees with the opportunity to gain knowledge of Incident Response (IR), Digital Forensics (DF), Reverse Engineering Malware (REM), Cyber Threat Intelligence (CTI), and Cyber Threat Hunting (CTH).

Obsidian 4n6 Station: Pre-Recorded - Obsidian 4n6: Creating a custom Velociraptor collector

Blue Team Village's Project Obsidian is an immersive, defensive cybersecurity learning experience that provides attendees with the opportunity to gain knowledge of Incident Response (IR), Digital Forensics (DF), Reverse Engineering Malware (REM), Cyber Threat Intelligence (CTI), and Cyber Threat Hunting (CTH).

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## BTV - Friday - 10:30-11:30 PDT

---

**Title:** Obsidian Forensics: Kill Chain 1 Endpoint Forensics Walkthrough

**When:** Friday, Aug 12, 10:30 - 11:30 PDT

**Where:** Flamingo - Savoy Ballroom - BTV Project Obsidian: Track 0x41

**SpeakerBio:** Omenscan

Obsidian Forensics Lead

### Description:

Obsidian Forensics Station: In this pre-recorded presentation we will walk through the artifacts and analysis of the Obsidian Kill Chain 1 using forensics artifacts found on the affected Endpoints.

Blue Team Village's Project Obsidian is an immersive, defensive cybersecurity learning experience that provides attendees with the opportunity to gain knowledge of Incident Response (IR), Digital Forensics (DF), Reverse Engineering Malware (REM), Cyber Threat Intelligence (CTI), and Cyber Threat Hunting (CTH).

Obsidian Forensics Station: Kill Chain 1 Endpoint Forensics Walkthrough

Blue Team Village's Project Obsidian is an immersive, defensive cybersecurity learning experience that provides attendees with the opportunity to gain knowledge of Incident Response (IR), Digital Forensics (DF), Reverse Engineering Malware (REM), Cyber Threat Intelligence (CTI), and Cyber Threat Hunting (CTH).

---

[Return to Index](#) - Add to



- ics [Calendar](#) file

## BTV - Saturday - 11:30-12:30 PDT

---

**Title:** Obsidian Forensics: Kill Chain 3 Endpoint Forensics Walkthrough

**When:** Saturday, Aug 13, 11:30 - 12:30 PDT

**Where:** Flamingo - Savoy Ballroom - BTV Project Obsidian: Track 0x41

**SpeakerBio:** Omenscan

Obsidian Forensics Lead

### Description:

Obsidian Forensics Station: In this pre-recorded presentation we will walk through the artifacts and analysis of the Obsidian Kill Chain 3 using forensics artifacts found on affected Endpoints.

Blue Team Village's Project Obsidian is an immersive, defensive cybersecurity learning experience that provides attendees with the opportunity to gain knowledge of Incident Response (IR), Digital Forensics (DF), Reverse Engineering Malware (REM), Cyber Threat Intelligence (CTI), and Cyber Threat Hunting (CTH).

Obsidian Forensics Station: Kill Chain 3 Endpoint Forensics Walkthrough

Blue Team Village's Project Obsidian is an immersive, defensive cybersecurity learning experience that provides attendees with the opportunity to gain knowledge of Incident Response (IR), Digital Forensics (DF), Reverse Engineering Malware (REM), Cyber Threat Intelligence (CTI), and Cyber Threat Hunting (CTH).

---

[Return to Index](#) - Add to



- ics [Calendar](#) file

## **BTV - Friday - 13:00-13:59 PDT**

---

**Title:** Obsidian Forensics: KillChain1 - Adventures in Splunk and Security Onion

**When:** Friday, Aug 12, 13:00 - 13:59 PDT

**Where:** Flamingo - Savoy Ballroom - BTV Main Stage

**Speakers:** ExtremePaperClip, Omenscan, Wes Lambert

**SpeakerBio:** ExtremePaperClip

Digital Forensics Nerd, Linux Geek, InfoSec Dork, Lifelong Student of Everything, Amateur History Buff... Loads of Fun.

**SpeakerBio:** Omenscan

Obsidian Forensics Lead

**SpeakerBio:** Wes Lambert

No BIO available

### **Description:**

A Live Forensics Walkthrough of Obsidian Kill Chain 1 (KC1) forensics analysis using Splunk and Security Onion

Blue Team Village's Project Obsidian is an immersive, defensive cybersecurity learning experience that provides attendees with the opportunity to gain knowledge of Incident Response (IR), Digital Forensics (DF), Reverse Engineering Malware (REM), Cyber Threat Intelligence (CTI), and Cyber Threat Hunting (CTH).

A Live Forensics Walkthrough of Obsidian Kill Chain 1 (KC1) forensics analysis using Splunk and Security Onion

Blue Team Village's Project Obsidian is an immersive, defensive cybersecurity learning experience that provides attendees with the opportunity to gain knowledge of Incident Response (IR), Digital Forensics (DF), Reverse Engineering Malware (REM), Cyber Threat Intelligence (CTI), and Cyber Threat Hunting (CTH).

---

[Return to Index](#) - Add to



- ics [Calendar](#) file

---

## **BTV - Saturday - 10:30-11:30 PDT**

---

**Title:** Obsidian Forensics: KillChain3 - Continued Adventures in Splunk and Security Onion

**When:** Saturday, Aug 13, 10:30 - 11:30 PDT

**Where:** Flamingo - Savoy Ballroom - BTV Main Stage

**Speakers:** Omenscan, Wes Lambert, ExtremePaperClip

**SpeakerBio:** Omenscan

Obsidian Forensics Lead

**SpeakerBio:** Wes Lambert

No BIO available

**SpeakerBio:** ExtremePaperClip

Digital Forensics Nerd, Linux Geek, InfoSec Dork, Lifelong Student of Everything, Amateur History Buff... Loads of Fun.

## Description:

A Live Forensics Walkthrough of Obsidian Kill Chain 3 (KC3) forensics analysis using Splunk and Security Onion

Blue Team Village's Project Obsidian is an immersive, defensive cybersecurity learning experience that provides attendees with the opportunity to gain knowledge of Incident Response (IR), Digital Forensics (DF), Reverse Engineering Malware (REM), Cyber Threat Intelligence (CTI), and Cyber Threat Hunting (CTH).

A Live Forensics Walkthrough of Obsidian Kill Chain 3 (KC3) forensics analysis using Splunk and Security Onion

Blue Team Village's Project Obsidian is an immersive, defensive cybersecurity learning experience that provides attendees with the opportunity to gain knowledge of Incident Response (IR), Digital Forensics (DF), Reverse Engineering Malware (REM), Cyber Threat Intelligence (CTI), and Cyber Threat Hunting (CTH).

[Return to Index](#) - Add to



- ics [Calendar](#) file

## BTV - Friday - 14:00-14:59 PDT

**Title:** Obsidian Forensics: The Importance of Sysmon for Investigations

**When:** Friday, Aug 12, 14:00 - 14:59 PDT

**Where:** Flamingo - Savoy Ballroom - BTV Project Obsidian: Track 0x41

**SpeakerBio:** ExtremePaperClip

Digital Forensics Nerd, Linux Geek, InfoSec Dork, Lifelong Student of Everything, Amateur History Buff... Loads of Fun.

### Description:

Video presentation outlining the benefits of Sysmon for investigations.

Blue Team Village's Project Obsidian is an immersive, defensive cybersecurity learning experience that provides attendees with the opportunity to gain knowledge of Incident Response (IR), Digital Forensics (DF), Reverse Engineering Malware (REM), Cyber Threat Intelligence (CTI), and Cyber Threat Hunting (CTH).

In this video we will discuss Sysmon -- what it is, how to get it, the configuration file, the events it logs, and why it's so valuable to forensic investigations.

Blue Team Village's Project Obsidian is an immersive, defensive cybersecurity learning experience that provides attendees with the opportunity to gain knowledge of Incident Response (IR), Digital Forensics (DF), Reverse Engineering Malware (REM), Cyber Threat Intelligence (CTI), and Cyber Threat Hunting (CTH).

[Return to Index](#) - Add to



- ics [Calendar](#) file

## BTV - Saturday - 14:00-14:59 PDT

**Title:** Obsidian Forensics: Using Chainsaw to Identify Malicious Activity

**When:** Saturday, Aug 13, 14:00 - 14:59 PDT

**Where:** Flamingo - Savoy Ballroom - BTV Project Obsidian: Track 0x41

**SpeakerBio:** Danny D. Henderson Jr (B4nd1t0)

With 14-years career in the U.S. public sector and 11 years with ICT, Danny now works at SecureWorks in Bucharest as an L3 SOC Analyst. His skillset includes digital forensics, threat intelligence, malware analysis, with small touch of Offensive Security. Outside of the Security field, Danny is working on a passion video game project as the Fearless Leader of the Sacred Star Team and is fond of fantasy tabletop games such as Dungeons and Dragons (D&D).

## Description:

This talk is a small in-depth look of using Chainsaw for investigations using the Obsidian project as the example.

The intent is to go over the following: - Default display to console

- Creating a CSV for slicing and to put into a spreadsheet - SIGMA rules and how Chinsaw applies those rules

Blue Team Village's Project Obsidian is an immersive, defensive cybersecurity learning experience that provides attendees with the opportunity to gain knowledge of Incident Response (IR), Digital Forensics (DF), Reverse Engineering Malware (REM), Cyber Threat Intelligence (CTI), and Cyber Threat Hunting (CTH).

When time is of essence in IR, having a tool to quickly collect data from Windows Event Logs is the way to go. We'll LET IT RIP with Chainsaw, hosted by B4nd1t0 as part of Project Obsidian.

Blue Team Village's Project Obsidian is an immersive, defensive cybersecurity learning experience that provides attendees with the opportunity to gain knowledge of Incident Response (IR), Digital Forensics (DF), Reverse Engineering Malware (REM), Cyber Threat Intelligence (CTI), and Cyber Threat Hunting (CTH).

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## BTV - Friday - 10:30-11:30 PDT

---

**Title:** Obsidian Live: Eating the Elephant 1 byte at a Time

**When:** Friday, Aug 12, 10:30 - 11:30 PDT

**Where:** Flamingo - Savoy Ballroom - BTV Main Stage

**Speakers:**aviditas,ChocolateCoat

**SpeakerBio:**aviditas

No BIO available

**SpeakerBio:**ChocolateCoat

No BIO available

## Description:

Incident Response: This is a live walkthrough of a real world incident focused on the first half of incident response. We will be breaking down scoping, triage, and communication aspects of incident handling into digestible and actionable recommendations.

Blue Team Village's Project Obsidian is an immersive, defensive cybersecurity learning experience that provides attendees with the opportunity to gain knowledge of Incident Response (IR), Digital Forensics (DF), Reverse Engineering Malware (REM), Cyber Threat Intelligence (CTI), and Cyber Threat Hunting (CTH).

Incident Response: This is a live walkthrough of a real world incident focused on the first half of incident response. We will be breaking down scoping, triage, and communication aspects of incident handling into digestible and actionable recommendations.

Blue Team Village's Project Obsidian is an immersive, defensive cybersecurity learning experience that provides attendees with the opportunity to gain knowledge of Incident Response (IR), Digital Forensics (DF), Reverse Engineering Malware (REM), Cyber Threat Intelligence (CTI), and Cyber Threat Hunting (CTH).

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## **BTV - Saturday - 14:00-14:59 PDT**

---

**Title:** Obsidian Live: May We Have the OODA Loops?

**When:** Saturday, Aug 13, 14:00 - 14:59 PDT

**Where:** Flamingo - Savoy Ballroom - BTV Main Stage

**Speakers:**CountZ3r0,juju43

**SpeakerBio:**CountZ3r0

Stuff goes here.

**SpeakerBio:**juju43

No BIO available

### **Description:**

Incident Response Live Walkthrough: This will go over how to use OODA to effectively investigate and respond to a real world incident. Come work through the demos alongside experts during this live walkthrough.

Blue Team Village's Project Obsidian is an immersive, defensive cybersecurity learning experience that provides attendees with the opportunity to gain knowledge of Incident Response (IR), Digital Forensics (DF), Reverse Engineering Malware (REM), Cyber Threat Intelligence (CTI), and Cyber Threat Hunting (CTH).

Incident Response Live Walkthrough: This will go over how to use OODA to effectively investigate and respond to a real world incident. Come work through the demos alongside experts during this live walkthrough.

Blue Team Village's Project Obsidian is an immersive, defensive cybersecurity learning experience that provides attendees with the opportunity to gain knowledge of Incident Response (IR), Digital Forensics (DF), Reverse Engineering Malware (REM), Cyber Threat Intelligence (CTI), and Cyber Threat Hunting (CTH).

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## **BTV - Friday - 14:00-14:59 PDT**

---

**Title:** Obsidian REM: Long Walks On The Beach: Analyzing Collected PowerShells

**When:** Friday, Aug 12, 14:00 - 14:59 PDT

**Where:** Flamingo - Savoy Ballroom - BTV Project Obsidian: Track 0x42

**SpeakerBio:**Alison N

No BIO available

### **Description:**

A quick introduction to malware analysis, Powershell script analysis, and how to not panic when VirusTotal shrugs.

Blue Team Village's Project Obsidian is an immersive, defensive cybersecurity learning experience that provides attendees with the opportunity to gain knowledge of Incident Response (IR), Digital Forensics (DF), Reverse Engineering Malware (REM), Cyber Threat Intelligence (CTI), and Cyber Threat Hunting (CTH).

So you just got a bunch of Powershell scripts dumped on you. What now?

Blue Team Village's Project Obsidian is an immersive, defensive cybersecurity learning experience that provides attendees with the opportunity to gain knowledge of Incident Response (IR), Digital Forensics (DF), Reverse Engineering Malware (REM), Cyber Threat Intelligence (CTI), and Cyber Threat Hunting (CTH).

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## **BTW - Saturday - 13:00-13:59 PDT**

---

**Title:** Obsidian REM: Phishing In The Morning: An Abundance of Samples!

**When:** Saturday, Aug 13, 13:00 - 13:59 PDT

**Where:** Flamingo - Savoy Ballroom - BTW Project Obsidian: Track 0x42

**SpeakerBio:** Alison N

No BIO available

### **Description:**

Coming soon

Coming soon

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## **BTW - Saturday - 13:00-13:59 PDT**

---

**Title:** Obsidian: IR - Final Reporting Made Exciting\*

**When:** Saturday, Aug 13, 13:00 - 13:59 PDT

**Where:** Flamingo - Savoy Ballroom - BTW Project Obsidian: Track 0x41

**Speakers:**aviditas,CountZ3r0

**SpeakerBio:**aviditas

No BIO available

**SpeakerBio:**CountZ3r0

Stuff goes here.

### **Description:**

\*Insert eye catching and compelling abstract on IR final reporting here. Make it seem exciting and not at all a dreaded yet critical part of incident handling.

Blue Team Village's Project Obsidian is an immersive, defensive cybersecurity learning experience that provides attendees with the opportunity to gain knowledge of Incident Response (IR), Digital Forensics (DF), Reverse Engineering Malware

(REM), Cyber Threat Intelligence (CTI), and Cyber Threat Hunting (CTH).

\*Insert eye catching and compelling abstract on IR final reporting here. Make it seem exciting and not at all a dreaded yet critical part of incident handling.

Blue Team Village's Project Obsidian is an immersive, defensive cybersecurity learning experience that provides attendees with the opportunity to gain knowledge of Incident Response (IR), Digital Forensics (DF), Reverse Engineering Malware (REM), Cyber Threat Intelligence (CTI), and Cyber Threat Hunting (CTH).

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## **BTW - Friday - 11:30-12:30 PDT**

---

**Title:** Obsidian: IR - It all starts here, scoping the incident

**When:** Friday, Aug 12, 11:30 - 12:30 PDT

**Where:** Flamingo - Savoy Ballroom - BTW Project Obsidian: Track 0x41

**SpeakerBio:**ChocolateCoat

No BIO available

### **Description:**

Scoping and Triage

You can't analyze what you don't know, learn to prepare yourself for any investigation no matter the subject.

Blue Team Village's Project Obsidian is an immersive, defensive cybersecurity learning experience that provides attendees with the opportunity to gain knowledge of Incident Response (IR), Digital Forensics (DF), Reverse Engineering Malware (REM), Cyber Threat Intelligence (CTI), and Cyber Threat Hunting (CTH).

You can't analyze what you don't know, learn to prepare yourself for any investigation no matter the subject.

Blue Team Village's Project Obsidian is an immersive, defensive cybersecurity learning experience that provides attendees with the opportunity to gain knowledge of Incident Response (IR), Digital Forensics (DF), Reverse Engineering Malware (REM), Cyber Threat Intelligence (CTI), and Cyber Threat Hunting (CTH).

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## **BTW - Friday - 13:00-13:59 PDT**

---

**Title:** Obsidian: IR - Mise En Place for Investigations

**When:** Friday, Aug 12, 13:00 - 13:59 PDT

**Where:** Flamingo - Savoy Ballroom - BTW Project Obsidian: Track 0x41

**Speakers:**aviditas,ChocolateCoat,CountZ3r0

**SpeakerBio:**aviditas

No BIO available

**SpeakerBio:**ChocolateCoat

No BIO available

**SpeakerBio:**CountZ3r0

Stuff goes here.

## Description:

Project Obsidian Incident Response station will walk through how to capture the necessary information as you are actively working an incident without slowing down on tickets, notes, timeline recording, and status updates. Plus tips based on years of IR experience on what NOT to do; spend less time writing and more time doing. This session is based on Kill Chain 1 data set and will show you how to prep and work an incident with a focus on communication and efficiency in all aspects.

Blue Team Village's Project Obsidian is an immersive, defensive cybersecurity learning experience that provides attendees with the opportunity to gain knowledge of Incident Response (IR), Digital Forensics (DF), Reverse Engineering Malware (REM), Cyber Threat Intelligence (CTI), and Cyber Threat Hunting (CTH).

If you don't document it, it didn't happen. A real world approach to IR communication.

Blue Team Village's Project Obsidian is an immersive, defensive cybersecurity learning experience that provides attendees with the opportunity to gain knowledge of Incident Response (IR), Digital Forensics (DF), Reverse Engineering Malware (REM), Cyber Threat Intelligence (CTI), and Cyber Threat Hunting (CTH).

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## BTW - Saturday - 10:30-11:30 PDT

---

**Title:** Obsidian: IR - OODA! An hour in incident responder life

**When:** Saturday, Aug 13, 10:30 - 11:30 PDT

**Where:** Flamingo - Savoy Ballroom - BTW Project Obsidian: Track 0x41

**SpeakerBio:**juju43

No BIO available

## Description:

Project Obsidian Incident Response station will walk through the OODA loop and Jupyter Notebooks to help you investigate, document and answer the key questions during incidents. This session is based on Kill Chain 3 data set and will leverage msticpy. Data, Notebook and Presentation will be made available after Defcon.

Blue Team Village's Project Obsidian is an immersive, defensive cybersecurity learning experience that provides attendees with the opportunity to gain knowledge of Incident Response (IR), Digital Forensics (DF), Reverse Engineering Malware (REM), Cyber Threat Intelligence (CTI), and Cyber Threat Hunting (CTH).

Let's dance and fly from dogfight to cyberworld. How to investigate and win against threats.

Blue Team Village's Project Obsidian is an immersive, defensive cybersecurity learning experience that provides attendees with the opportunity to gain knowledge of Incident Response (IR), Digital Forensics (DF), Reverse Engineering Malware (REM), Cyber Threat Intelligence (CTI), and Cyber Threat Hunting (CTH).

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

**Title:** Off the grid - Supplying your own power

**When:** Sunday, Aug 14, 12:30 - 12:59 PDT

**Where:** Flamingo - Virginia City II

**SpeakerBio:**Eric Escobar

Eric is a seasoned pentester and a Security Principal Consultant at Secureworks. 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, 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!

Twitter: [@https://twitter.com/EricEscobar](https://twitter.com/EricEscobar)

**Description:**

Ever want to take your rig off-grid powered by only the sun an a variety of batteries? This talk will discuss how to operate low power off the grid indefinitely as well as considerations to make on batteries. We'll talk power, cables, batteries, crimping and more. Every ham has unique use cases, and this talk will allow you to tailor your kit to your off-grid needs!

---

[Return to Index](#) - Add to



- ics [Calendar](#) file

---

## PLV - Sunday - 12:00-13:45 PDT

---

**Title:** Offensive Cyber Industry Roundtable

**When:** Sunday, Aug 14, 12:00 - 13:45 PDT

**Where:** Caesars Forum - Summit 224-225 - Policy Collaboratorium

**Speakers:**Sophia D'Antoine,Winnona DeSombre,Matt Holland

**SpeakerBio:**Sophia D'Antoine , Founder of Margin Research

No BIO available

**SpeakerBio:**Winnona DeSombre

No BIO available

**SpeakerBio:**Matt Holland , Founder of Field Effect

No BIO available

**Description:**

Join us for a Chatham House Rule conversation with hackers that provide capabilities to government cyber operations. Learn about the development and sale of offensive cyber capabilities, and what the government/policy perspectives are for regulating this space.

---

[Return to Index](#) - Add to



- ics [Calendar](#) file

---

**Title:** Offensive IoT Exploitation

**When:** Tuesday, Aug 16, 09:00 - 16:59 PDT

**Where:** Caesars Forum

**Speakers:**Trevor Stevado,Trevor Hough,Patrick Ross,Nicholas Coad

**SpeakerBio:**Trevor Stevado

- 12+ years in offensive application and network security • Led and contributed to over 100 security assessments (Red Team, VA, Pen Test) • DEF CON 26 Black Badge holder (part of 3-person team) • Leads Pros versus Joes (PvJ) Red Cell • Founding Partner & Hacker @ Loudmouth Security

**SpeakerBio:**Trevor Hough

- 10+ years in offensive application and network security • Led and contributed to dozens of security assessments (Red Team, VA, Pen Test) • DEF CON 26 Black Badge holder (part of 3-person team) • Member of Pros versus Joes (PvJ) Red Cell • Managing Partner & Hacker @ Loudmouth Security

**SpeakerBio:**Patrick Ross

- 7+ years in offensive security roles
- 10+ years in security architecture
- DEF CON 26 Black Badge holder (part of 3-person team) • Member of Pros versus Joes (PvJ) Red Cell • Hacker @ Village Idiot Labs

**SpeakerBio:**Nicholas Coad

- 5+ years in offensive application and network security • 10+ years in network administration and security operations • Contributed to dozens of security assessments (Red Team, VA, Pen Test) • Managed security operations for Fortune 500 company • Winner of the IoT CTF, DEF CON 27
- Member of Pros versus Joes (PvJ) Red Cell • Hacker @ Loudmouth Security

## Description:

Latest details, requirements, description, cost:

<https://defcontrainings.myshopify.com/products/trevor-stevado-trevor-hough-nicholas-coad-patrick-ross-offensive-iot-exploitation>

Training description:

As IoT becomes more integrated and integral into personal and work lives, there is a growing need to understand the inner workings of IoT devices. The base skills required are the same as many other security disciplines, whether the task is to perform defensive-based penetration testing or gain covert access for evidence or intelligence collection. Testing IoT devices for security bridges several skill sets from application security, operating systems penetration testing, wireless signals analysis, and embedded hardware security. Unfortunately, many courses in this industry deal with each topic individually, either taking a deep dive into hardware hacking, teaching advanced web application security, or teaching exploit development of different microarchitectures. This training is curated to take a step back and look at the bigger picture of IoT security testing, teaching the basics of each skill set to bridge the gaps and enable students to apply modern penetration testing techniques to IoT devices.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

**Title:** Offensive IoT Exploitation

**When:** Monday, Aug 15, 09:00 - 16:59 PDT

**Where:** Caesars Forum

**Speakers:**Trevor Stevado,Trevor Hough,Patrick Ross,Nicholas Coad

**SpeakerBio:**Trevor Stevado

- 12+ years in offensive application and network security • Led and contributed to over 100 security assessments (Red Team, VA, Pen Test) • DEF CON 26 Black Badge holder (part of 3-person team) • Leads Pros versus Joes (PvJ) Red Cell • Founding Partner & Hacker @ Loudmouth Security

**SpeakerBio:**Trevor Hough

- 10+ years in offensive application and network security • Led and contributed to dozens of security assessments (Red Team, VA, Pen Test) • DEF CON 26 Black Badge holder (part of 3-person team) • Member of Pros versus Joes (PvJ) Red Cell • Managing Partner & Hacker @ Loudmouth Security

**SpeakerBio:**Patrick Ross

- 7+ years in offensive security roles
- 10+ years in security architecture
- DEF CON 26 Black Badge holder (part of 3-person team) • Member of Pros versus Joes (PvJ) Red Cell • Hacker @ Village Idiot Labs

**SpeakerBio:**Nicholas Coad

- 5+ years in offensive application and network security • 10+ years in network administration and security operations • Contributed to dozens of security assessments (Red Team, VA, Pen Test) • Managed security operations for Fortune 500 company • Winner of the IoT CTF, DEF CON 27
- Member of Pros versus Joes (PvJ) Red Cell • Hacker @ Loudmouth Security

## Description:

Latest details, requirements, description, cost:

<https://defcontrainings.myshopify.com/products/trevor-stevado-trevor-hough-nicholas-coad-patrick-ross-offensive-iot-exploitation>

Training description:

As IoT becomes more integrated and integral into personal and work lives, there is a growing need to understand the inner workings of IoT devices. The base skills required are the same as many other security disciplines, whether the task is to perform defensive-based penetration testing or gain covert access for evidence or intelligence collection. Testing IoT devices for security bridges several skill sets from application security, operating systems penetration testing, wireless signals analysis, and embedded hardware security. Unfortunately, many courses in this industry deal with each topic individually, either taking a deep dive into hardware hacking, teaching advanced web application security, or teaching exploit development of different microarchitectures. This training is curated to take a step back and look at the bigger picture of IoT security testing, teaching the basics of each skill set to bridge the gaps and enable students to apply modern penetration testing techniques to IoT devices.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

## DC - Friday - 10:00-10:45 PDT

---

**Title:** Old Malware, New tools: Ghidra and Commodore 64, why understanding old malicious software still matters

**When:** Friday, Aug 12, 10:00 - 10:45 PDT

**Where:** Caesars Forum - Academy 401-410, 421 (Track 3)

**SpeakerBio:** Cesare Pizzi , Hacker

Cesare Pizzi is a Security Researcher, Analyst, and Technology Enthusiast at Sorint.lab.

He develops software and hardware, and tries to share this with the community. Mainly focused on low level programming, he develops and contributes to OpenSource software (Volatility, OpenCanary, Cetus, etc), sometimes hardware related (to interface some real world devices) sometimes not. Doing a lot of reverse engineering too, so he feels confident in both "breaking" and "building" (may be more on breaking?).

Twitter: [@https://twitter.com/red5heep](https://twitter.com/red5heep)

### Description:

Why looking into a 30 years old "malicious" software make sense in 2022? Because this little "jewels", written in a bunch of bytes, reached a level of complexity surprisingly high. With no other reason than pranking people or show off technical knowledge, this software show how much you can do with very limited resources: this is inspiring for us, looking at modern malicious software, looking at how things are done and how the same things could have been done instead.

---

[Return to Index](#) - Add to



- ics [Calendar](#) file

---

## HRV - Sunday - 11:00-11:30 PDT

---

**Title:** Oli: A Simpler Pi-Star Replacement

**When:** Sunday, Aug 14, 11:00 - 11:30 PDT

**Where:** Flamingo - Virginia City II

**SpeakerBio:**Danny Quist

Danny Quist is an extra class amateur radio operator. He was first licensed in 1994 and enjoys CW, FT8, DMR, Dstar, and YSF operations. Aside from radio, Danny is a reverse engineer. He has spoken at Blackhat, Defcon, Shmoocon, Recon, and other conferences about reverse engineering topics.

### Description:

Oli: A Pi-Star replacement rewritten from scratch. DMR, Dstar, and other digital voice modes have long been the exclusive domain of Pi-Star. While a workhorse, there are many complicated settings to navigate before being able to make the first contact. This talk will discuss Oli, a project built from the ground up to be fast and pleasant to use. This will be a live demo and tool release.

---

[Return to Index](#) - Add to



- ics [Calendar](#) file

---

## CPV - Friday - 16:00-16:45 PDT

---

**Title:** Once More Unto the Breach: Federal Regulators' Response to Privacy Breaches and Consumer Harms

**When:** Friday, Aug 12, 16:00 - 16:45 PDT

**Where:** Flamingo - Vista Ballroom

**Speakers:**Erie Meyer,Alexis Goldstein

### **SpeakerBio:**Erie Meyer

Erie Meyer is the Chief Technologist at the Consumer Financial Protection Bureau (CFPB). Most recently, she served as Senior Advisor to Chair Khan for Policy Planning and Chief Technologist for the Federal Trade Commission, and as then-Commissioner Chopra's Technology Advisor. Before serving at the FTC, she launched the U.S. Digital Service in the White House. Ms. Meyer has also served as Senior Director for Code for America and Senior Advisor to the White House's Chief Technology Officer. Ms. Meyer is co-founder of Tech Ladymafia, and she is a recipient of the Harvard Kennedy School's Joan Shorenstein Fellowship during which she researched the intersection of open data, journalism, and civic life. Ms. Meyer is a contributor to open source software and received her B.A. in journalism from American University.

### **SpeakerBio:**Alexis Goldstein

No BIO available

### **Description:**

When consumers' data is pwned, what are the legal and regulatory tools available? Consumer harms result not only from explicit privacy violations, but also from inadequate data security. We will walk through several relevant laws and regulations, as well as past cases where firms were held accountable. We will also examine past remedies that tackled the harms and attempted to prevent them going forward.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## **DC - Friday - 12:00-12:45 PDT**

---

**Title:** One Bootloader to Load Them All

**When:** Friday, Aug 12, 12:00 - 12:45 PDT

**Where:** Caesars Forum - Alliance 301-309, 321 (Track 4)

**Speakers:**Jesse Michael,Mickey Shkatov

### **SpeakerBio:**Jesse Michael , Hacker

Jesse Michael - 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.

Twitter: [@https://twitter.com/JesseMichael](https://twitter.com/JesseMichael)

### **SpeakerBio:**Mickey Shkatov , Hacker

Mickey has been doing security research for almost a decade, one of specialties is simplifying complex concepts and finding security flaws in unlikely places. He has seen some crazy things and lived to tell about them at security conferences all over the world, his past talks range from web pentesting to black badges and from hacking cars to BIOS firmware.

Twitter: [@https://twitter.com/HackingThings](https://twitter.com/HackingThings)

### **Description:**

Introduced in 2012, Secure Boot - the OG trust in boot - has become a foundational rock in modern computing and is used by millions of UEFI-enabled computers around the world due to its integration in their BIOS. The way Secure Boot works is simple and effective, by using tightly controlled code signing certificates, OEMs like Microsoft, Lenovo, Dell and others secure their boot process, blocking unsigned code from running during boot. But this model puts its trust in developers developing code without vulnerabilities or backdoors; in this presentation we will discuss past and current flaws in valid

bootloaders, including some which misuse built-in features to inadvertently bypass Secure Boot. We will also discuss how in some cases malicious executables can hide from TPM measurements used by BitLocker and remote attestation mechanisms. Come join us as we dive deeper and explain how it all works, describe the vulnerabilities we found and walk you through how to use the new exploits and custom tools we created to allow for a consistent bypass for secure boot effective against every X86-64 UEFI platform.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## DC - Friday - 10:30-11:15 PDT

---

**Title:** OpsSec -The bad, the worst and the ugly of APT's operations security

**When:** Friday, Aug 12, 10:30 - 11:15 PDT

**Where:** Caesars Forum - Alliance 301-309, 321 (Track 4)

**SpeakerBio:** Tomer Bar , Director of Security Research at SafeBreach

Tomer Bar is a hands-on security researcher with ~20 years of unique experience in cyber security. In the past, he ran research groups for the Israeli government and then led the endpoint malware research for Palo Alto Networks. Currently, he leads the SafeBreach Labs as the director of security research.

His main interests are Windows vulnerability research, reverse engineering, and APT research.

His recent discoveries are the PrintDemon vulnerabilities in the Windows Spooler mechanism which were a candidate in the best privilege escalation of 2021 Pwnie awards and several research studies on Iranian APT campaigns.

He is a contributor to the MITRE ATT&CK® framework.

He presented his research at BlackHat 2020, Defcon 2020, 2021, and Sector 2020 conferences.

### Description:

Advanced Persistent Threat groups invest in developing their arsenal of exploits and malware to stay below the radar and persist on the target machines for as long as possible. We were curious if the same efforts are invested in the operation security of these campaigns. We started a journey researching active campaigns from the Middle East to the Far East including the Palestinian Authority, Turkey, and Iran, Russia, China, and North Korea. These campaigns were both state-sponsored, surveillance-targeted attacks and large-scale financially-motivated attacks. We analyzed every technology used throughout the attack chain: Windows (Go-lang/.Net/Delphi) and Android malware; both on Windows and Linux-based C2 servers. We found unbelievable mistakes which allow us to discover new advanced TTPs used by attackers, for example: bypassing iCloud two-factor authentication' and crypto wallet and NFT stealing methods. We were able to join the attackers' internal groups, view their chats, bank accounts and crypto wallets. In some cases, we were able to take down the entire campaign. We will present our latest breakthroughs from our seven-year mind-game against the sophisticated Infy threat actor who successfully ran a 15-year active campaign using the most secured opSec attack chain we've encountered. We will explain how they improved their opSec over the years and how we recently managed to monitor their activity and could even cause a large-scale misinformation counterattack. We will conclude by explaining how organizations can better defend themselves.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## CPV - Friday - 11:30-11:59 PDT

---

**Title:** OPAQUE is Not Magic

**When:** Friday, Aug 12, 11:30 - 11:59 PDT

**Where:** Flamingo - Vista Ballroom

### **SpeakerBio:**Steve Thomas

Steve Thomas, aka Sc00bz, is a cryptography enthusiast and specializes on the defensive side of passwords. His current focus is in PAKEs and key stretching for aPAKEs. He was on the Password Hashing Competition's panel that ultimately picked Argon2. He was break two of the submissions with one being fixable. "I do stuff... sometimes."

### **Description:**

Dispelling myths about OPAQUE. What OPAQUE is and more importantly what it is not. The RFC for OPAQUE is not finalized and people are already implementing it and running into its footgun. Are there better and/or faster PAKEs? The types of PAKEs (balanced, augmented, double augmented, and identity) and what they are used for. PAKEs are just AKEs (authenticated key exchanges) with something hidden with a password. The properties of PAKEs: forward secrecy, fragile, quantum annoying, prevent precomputation, secure registration, and number of trips.

---

[Return to Index](#) - Add to



- ics [Calendar](#) file

---

## **DC - Saturday - 14:00-14:45 PDT**

---

**Title:** OpenCola. The AntiSocial Network

**When:** Saturday, Aug 13, 14:00 - 14:45 PDT

**Where:** Caesars Forum - Forum 104-105, 135-136 (Track 1)

### **SpeakerBio:**John Midgley , Cult of the Dead Cow

John Midgley was born and raised in Toronto, Canada. He studied computer science at the University of Toronto where he earned a B.Sc. and a Masters in Computer Vision. His first job out of school was building the search algorithms for openCola, an early peer to peer collaboration tool that was arguably 20 years ahead of its time. Not being able to afford a time machine, he busied himself by working at a string of startups and then a couple larger companies (Microsoft and Netflix). From 2011 to 2021 he worked at Netflix on Facebook integration, search, video ranking, content promotion and ended up managing the personalization organization, responsible for the systems and algorithms that construct the Netflix experience. Now that it's 20 years later, the world may finally be ready for a new and improved version of OpenCola.

### **Description:**

The internet, as it stands today, is not a very trustworthy environment, as evidenced by the numerous headlines of companies abusing personal data and activity. This is not really surprising since companies are responsible for optimizing revenue, which is often at odds with user benefit. The result of these incentives has produced or exacerbated significant problems: tech silos, misinformation, privacy abuse, concentration of wealth, the attention economy, etc. We built OpenCola, free and open source, as an alternative to existing big-tech applications. It puts users in control of their personal activity and the algorithms that shape the flow of data to them. We believe that this solution, although simple, can significantly mitigate the challenges facing the Internet.

---

[Return to Index](#) - Add to



- ics [Calendar](#) file

---

## **AIV - Friday - 09:00-09:25 PDT**

---

**Title:** Opening Remarks on the State of AI & Security

**When:** Friday, Aug 12, 09:00 - 09:25 PDT

**Where:** Caesars Forum - Summit 228->236

**Speakers:**Brian Pendleton,Sven Cattell

**SpeakerBio:**Brian Pendleton

No BIO available

Twitter: [@https://twitter.com/yaganub](https://twitter.com/yaganub)

**SpeakerBio:**Sven Cattell

No BIO available

Twitter: [@https://twitter.com/comathematician](https://twitter.com/comathematician)

**Description:**No Description available

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## DL - Saturday - 14:00-15:55 PDT

---

**Title:** OpenTDF

**When:** Saturday, Aug 13, 14:00 - 15:55 PDT

**Where:** Caesars Forum - Accord Boardroom

**Speakers:**Paul Flynn,Cassandra Bailey

**SpeakerBio:**Paul Flynn

Paul has been a software developer for over 25 years, starting as a webmaster in 1995. Paul has worked on securely connecting merchants with banking mainframes; providing governments with digital signing and receipting of documents, and solved Y2K. He has helped scale some of the largest web sites of its time (eBay, Obamacare) and worked on command-and-control systems of life-saving McMurdo beacons. Paul has recognized the deficiency of security from his past and is proud of the solution that is available in OpenTDF.

**SpeakerBio:**Cassandra Bailey

Cassandra started her career as a full-stack developer for web and macOS applications, and has since managed projects and products in the DeFi, gaming, and most recently, data protection and security spaces. The latter corresponds to her role in helping to develop and manage the OpenTDF project, an open-source API and SDK that leverages the Trusted Data Format (TDF) to enable zero-trust data protection.

**Description:**

OpenTDF is an open source project that provides developers with the tools to build data protections natively within their applications using the Trusted Data Format (TDF).

Audience: AppSec, Defense, Mobile, IoT

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## BHV - Saturday - 13:00-13:30 PDT

---

**Title:** Out of the Abyss: Surviving Vulnerability Management

**When:** Saturday, Aug 13, 13:00 - 13:30 PDT

**Where:** Flamingo - Laughlin I,II,III

**Speakers:** Leo Nendza, Mike Kijewski

**SpeakerBio:** Leo Nendza

Leo is a Senior Software Development Engineer on MedCrypt's Heimdall project and a forever DM.

**SpeakerBio:** Mike Kijewski

Mike is the cofounder of MedCrypt, a medical device cybersecurity startup based in San Diego, CA.

Twitter: [@https://twitter.com/mikekijewski](https://twitter.com/mikekijewski)

### Description:

""The introduction of an SBOM in the 2018 FDA premarket cybersecurity guidance, and inclusion in update 2022 quality system considerations guidance, has become a rallying cry for SBOM adoption across the healthcare industry. However, three years on and progress has been incremental in generation, adoption, distribution and consumption. The end objective is knowing when a vulnerability impacts an ecosystem.

This talk shares some observations, practical / technical insights into challenges, and paints a picture of the potential future we could have."""

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## CPV - Friday - 16:45-17:30 PDT

---

**Title:** Owned or pwned? No peakin' or tweakin'!

**When:** Friday, Aug 12, 16:45 - 17:30 PDT

**Where:** Flamingo - Vista Ballroom

**Speakers:** Nick Vidal, Richard Zak

**SpeakerBio:** Nick Vidal

Nick Vidal is the Community Manager of Profian and the Enarx project, which is part of the Confidential Computing Consortium from the Linux Foundation. Previously, he was the Director of Community and Business Development at the Open Source Initiative, Director of Americas at the Open Invention Network, and one of the community leaders of the Drupal project in Latin America

**SpeakerBio:** Richard Zak

After a decade of malware and machine learning research, and publishing several papers, Richard decided to switch gears and work on Enarx and Confidential Computing. He is also a part-time computer science instructor at a university. Outside of work, he enjoys working on open source projects, playing video games, and tinkering with various technologies. Website: <https://rjzak.github.io/>

### Description:

The Cloud is just somebody else's computer. So when you run a workload on a cloud host, anyone who owns (or pwns) that system can peak or tweak the data or even the application itself. You have no confidentiality or integrity protection from your Cloud Service Provider, rogue sysadmins, or just anyone who compromises their machines.

But being pwned does not necessarily mean it's endgame. Confidential Computing uses hardware-based Trusted Execution Environments to provide confidentiality and integrity even in the most vulnerable scenarios.

This session will define Confidential Computing at a technical level and discuss current and upcoming hardware that have support for it. Later, we'll introduce Enarx, an open source Linux Foundation project, and present a live demo to showcase Confidential Computing in a system that has been "pwned."

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## DL - Friday - 12:00-13:55 PDT

---

**Title:** Packet Sender

**When:** Friday, Aug 12, 12:00 - 13:55 PDT

**Where:** Caesars Forum - Accord Boardroom

**SpeakerBio:**Dan Nagle

Dan Nagle has over 15 years of software development experience. He has written and published apps for desktop, mobile, servers, and embedded. He is the author and inventor of Packet Sender, an app used daily by security researchers, featured in manuals from major tech companies, and is taught in universities around the world. He is also the author of 2 network-related patents and a book published by CRC Press. His open source contributions have received international awards, and he has presented at many developer conferences about them.

### Description:

Packet Sender is a free open-source (GPLv2) cross-platform (Windows, Mac, Linux) tool used daily by security researchers, college students, and professional developers to troubleshoot and reverse engineer network-based devices. Its core features are crafting and listening for UDP, TCP, and SSL/TLS packets via IPv4 or IPv6. It can listen simultaneously on any number of ports while sending to any UDP, TCP, SSL/TLS packet server. It is available for direct download or through the Winget, Homebrew, Debian, or Snap repos.

Audience: Offensive, Defensive, Developers, Testers

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## DC - Friday - 10:00-10:45 PDT

---

**Title:** Panel - "So It's your first DEF CON" - How to get the most out of DEF CON, What NOT to do.

**When:** Friday, Aug 12, 10:00 - 10:45 PDT

**Where:** Caesars Forum - Forum 104-105, 135-136 (Track 1)

**SpeakerBio:**DEF CON Goons

No BIO available

### Description:

Panel - "So It's your first DEF CON" - How to get the most out of DEF CON, What NOT to do. This talk is a guide to enjoying DEF CON. We hope to talk about how to get the most out of your first con and answer questions live from the audience. Feel free to come meet some long time goons, attendees, and DEF CON staff as we discuss how to navigate Las Vegas hotels with 30k hackers surrounding around you.

---

## DC - Friday - 10:00-11:15 PDT

---

**Title:** Panel - DEF CON Policy Dept - What is it, and what are we trying to do for hackers in the policy world?

**When:** Friday, Aug 12, 10:00 - 11:15 PDT

**Where:** Caesars Forum - Forum 106-110, 138-139 (Track 2)

**SpeakerBio:**DEF CON Policy Dept

No BIO available

### Description:

DEF CON Policy Dept - What is it, and what are we trying to do for hackers in the policy world?

---

## HRV - Saturday - 15:00-15:30 PDT

---

**Title:** Panel: Ask-a-ham

**When:** Saturday, Aug 13, 15:00 - 15:30 PDT

**Where:** Flamingo - Virginia City II

### Description:

Do you have any questions for those that have been involved in the amateur radio hobby? Now is the time to "Ask-A-Ham"!

---

## DL - Friday - 14:00-15:55 PDT

---

**Title:** PCILeech and MemProcFS

**When:** Friday, Aug 12, 14:00 - 15:55 PDT

**Where:** Caesars Forum - Council Boardroom

**Speakers:**Ian Vitek,Ulf Frisk

**SpeakerBio:**Ian Vitek

Ian Vitek has a background as a pentester but now works with information security in the Swedish financial sector. Ian has held several presentations at DEF CON, BSidesLV and other IT security conferences.

**SpeakerBio:**Ulf Frisk

Ulf is a pentester by day, and a security researcher by night. Ulf is the author of the PCILeech direct memory access attack toolkit and MemProcFS. Ulf is interested in things low-level and primarily focuses on memory analysis and DMA.

### Description:

The PCILeech direct memory access attack toolkit was presented at DEF CON 24 and quickly became popular amongst red

teamers and game hackers alike. We will demonstrate how to take control of still vulnerable systems with PCIe DMA code injection using affordable FPGA hardware and the open source PCILeech toolkit. MemProcFS is memory forensics and analysis made super easy! Analyze memory by clicking on files in a virtual file system or by using the API. Analyze memory dump files or live memory acquired using drivers or PCILeech PCIe FPGA hardware devices.

Audience: Offense, Defense, Forensics, Hardware

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## ASV - Friday - 16:00-16:50 PDT

---

**Title:** Pen Test Partner Power Hour

**When:** Friday, Aug 12, 16:00 - 16:50 PDT

**Where:** Caesars Forum - Forum 112-117

**Speakers:**Ken Munro,Alex Lomas

### **SpeakerBio:**Ken Munro , Pentes Partners

Ken Munro is Partner and Founder of Pen Test Partners, a firm of penetration testers with a keen interest in aviation. Pen Test Partners has several pilots on the team, both private and commercial, recognizing that the increase in retired airframes has created opportunities for independent security research into aviation security. Pen Test Partners has been recognized for its highly responsible approach to vulnerability disclosure in aviation and was invited to join the Boeing Cyber Technical Council as a result. Pen Test Partners has published research into aviation cyber security, covering topics from airborne connectivity, avionics hardware, and connectivity with ground systems.

### **SpeakerBio:**Alex Lomas

Alex Lomas is Pen Test Partner's aerospace specialist. Alex undertakes penetration testing of complex embedded systems including airport operational technology and avionics systems such as inflight entertainment and aircraft monitoring systems. Alex has a Masters in Aeronautical Engineering and has held a private pilot's license since 2011. These, combined with cyber security experience in both offensive and defensive roles, gives them a unique perspective when approaching the testing of airlines, airports, and aeronautical service providers.

### **Description:**

"Hacking EFBs: What's an EFB and how does hacking one affect flight safety? We'll cover tampering with perf, W&B and detail numerous real incidents that have stemmed from EFB misuse or miskeying. So far we've found exploitable vulns in 6 different EFB app suites, covering nearly every major operator in the world. Separately, the flight sim will be set up to demonstrate a tailstrike and/or runway excursion as a result of tampered perf on our own EFB" Vulnerability disclosure in aviation: the good, the bad and the unsafe:

"We've been researching aviation security for the past 5 years. Along the way we have responsibility disclosed numerous vulnerabilities. Our experience with various aviation businesses has ranged from excellent to appalling. Many of the issues stem from cultural issues at these businesses, failing to bust safety silos in engineering. What can anyone in aviation learn from our experience? How can one build a successful vulnerability disclosure program that boosts safety?"

Getting started in aviation & avionics security research

"Independent research in aviation has one big barrier to entry: airplanes cost \$millions! How does a researcher or research group break in past this barrier? We'll talk about ways we have successfully (and legally!) carried out vanilla security research in airplanes. What will you find on board and how do the various systems work?"

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## **ASV - Friday - 10:00-11:59 PDT**

---

**Title:** Pen Test Partners A320 Simulator

**When:** Friday, Aug 12, 10:00 - 11:59 PDT

**Where:** Caesars Forum - Forum 112-117

### **Description:**

Come take the controls of Pen Test Partners' immersive A320 simulator. Experience the effects of tampered electronic flight bag data on take-off and landing, TCAS spoofing and more all in the safety of the sim. You'll see how experienced pilots would deal with these incidents and mitigate risk to passengers and the airplane.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## **ASV - Friday - 13:00-14:59 PDT**

---

**Title:** Pen Test Partners A320 Simulator

**When:** Friday, Aug 12, 13:00 - 14:59 PDT

**Where:** Caesars Forum - Forum 112-117

### **Description:**

Come take the controls of Pen Test Partners' immersive A320 simulator. Experience the effects of tampered electronic flight bag data on take-off and landing, TCAS spoofing and more all in the safety of the sim. You'll see how experienced pilots would deal with these incidents and mitigate risk to passengers and the airplane.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## **ASV - Saturday - 10:00-11:59 PDT**

---

**Title:** Pen Test Partners A320 Simulator

**When:** Saturday, Aug 13, 10:00 - 11:59 PDT

**Where:** Caesars Forum - Forum 112-117

### **Description:**

Come take the controls of Pen Test Partners' immersive A320 simulator. Experience the effects of tampered electronic flight bag data on take-off and landing, TCAS spoofing and more all in the safety of the sim. You'll see how experienced pilots would deal with these incidents and mitigate risk to passengers and the airplane.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## **ASV - Saturday - 13:00-14:59 PDT**

---

**Title:** Pen Test Partners A320 Simulator

**When:** Saturday, Aug 13, 13:00 - 14:59 PDT

**Where:** Caesars Forum - Forum 112-117

### Description:

Come take the controls of Pen Test Partners' immersive A320 simulator. Experience the effects of tampered electronic flight bag data on take-off and landing, TCAS spoofing and more all in the safety of the sim. You'll see how experienced pilots would deal with these incidents and mitigate risk to passengers and the airplane.

[Return to Index](#) - Add to



- ics [Calendar](#) file

## ASV - Sunday - 10:00-11:59 PDT

**Title:** Pen Test Partners A320 Simulator

**When:** Sunday, Aug 14, 10:00 - 11:59 PDT

**Where:** Caesars Forum - Forum 112-117

### Description:

Come take the controls of Pen Test Partners' immersive A320 simulator. Experience the effects of tampered electronic flight bag data on take-off and landing, TCAS spoofing and more all in the safety of the sim. You'll see how experienced pilots would deal with these incidents and mitigate risk to passengers and the airplane.

[Return to Index](#) - Add to



- ics [Calendar](#) file

## WS - Thursday - 15:00-18:59 PDT

**Title:** Pentesting Industrial Control Systems 101: Capture the Flag!

**When:** Thursday, Aug 11, 15:00 - 18:59 PDT

**Where:** Harrah's - Ely

**Speakers:** Arnaud Soullie, Alexandrine Torrents

### SpeakerBio: Arnaud Soullie , Senior Manager

Arnaud Soullié (@arnaudsoullie) is a Senior Manager at Wavestone, a global consulting company. For 12 years, he has been performing security assessments and pentests on all types of targets. He started specializing in ICS cybersecurity 10 years ago. He spoke and taught workshops at numerous security conferences on ICS topics : BlackHat Europe, BruCon, CS3STHLM, BSides Las Vegas, DEFCON... He is also the creator of the DYODE project, an open-source data diode aimed at ICS. He has been teaching ICS cybersecurity training since 2015.

Twitter: [@https://twitter.com/arnaudsoullie](https://twitter.com/arnaudsoullie)

### SpeakerBio: Alexandrine Torrents , Security Consultant

Alexandrine Torrents is a cybersecurity consultant at Wavestone, a French consulting company. She started as a penetration tester, and performed several cybersecurity assessments on ICS. She worked on a few ICS models to demonstrate attacks on PLCs and developed a particular tool to request Siemens PLCs. Then, she started working at securing ICS, especially in the scope of the French military law, helping companies offering a vital service to the nation to comply with security rules. Now, Alexandrine works with different industrial CISOs on their cybersecurity projects: defining secure architectures, hardening systems, implementing detection mechanisms. She is also IEC 62443 certified and still performs assessments on multiple environments.

## Description:

Do you want to learn how to hack Industrial Control Systems? Let's participate in the one and only CTF in which you really have to capture a flag, by hacking PLCs and taking control of a robotic arm! We'll start by explaining the basics of Industrial Control Systems : what are the components, how they work, the protocols they use... We'll learn how PLC work, how to program them, and how to communicate with them using Modbus, S7comm and OPCUA.

Then we'll start hacking! Your goal will be to take control of a model train and robotic arms to capture a real flag! The CTF will be guided so that everyone learns something and gets a chance to get most flags!

## Materials

Just a laptop with a modern web browser. Students will be provided with cloud VMs to perform the exercises.

## Prereq

None

---

[Return to Index](#) - Add to



- ics [Calendar](#) file

---

## DC - Saturday - 15:30-16:15 PDT

---

**Title:** Perimeter Breached! Hacking an Access Control System

**When:** Saturday, Aug 13, 15:30 - 16:15 PDT

**Where:** Caesars Forum - Alliance 301-309, 321 (Track 4)

**Speakers:** Sam Quinn, Steve Povolny

### **SpeakerBio:** Sam Quinn , Senior Security Researcher

Sam Quinn, @eAyeP, is a Senior Security Researcher on the Advanced Threat Research team, focused on finding new vulnerabilities in both software and hardware. Sam has a focus on embedded devices with knowledge in the fields of reverse engineering and exploitation. He has had numerous vulnerability findings and published CVEs in the areas of IOT and enterprise software.

Twitter: <https://twitter.com/eAyeP>

### **SpeakerBio:** Steve Povolny , Principal Engineer & Head of Advanced Threat Research

Steve Povolny, @spovolny, is the Head of Advanced Threat Research for Trellix, which delivers groundbreaking vulnerability research spanning nearly every industry. With more than a decade of experience in network security, Steve is a recognized authority on hardware and software vulnerabilities, and regularly collaborates with influencers in academia, government, law enforcement, consumers and enterprise businesses of all sizes. Steve is a sought after public speaker and media commentator who often blogs on key topics. He brings his passion for threat research and a unique vision to harness the power of collaboration between the research community and product vendors, through responsible disclosure, for the benefit of all.

Twitter: <https://twitter.com/spovolny>

## Description:

The first critical component to any attack is an entry point. As we lock down firewalls and routers, it can be easy to overlook the network-connected physical access control systems. A study done by IBM in 2021 showed that the average cost of a physical security compromise is \$3.54 million and takes an average of 223 days to identify a breach.

HID Mercury is a global distributor of access control systems with more than 20 OEM partners, deployed across multiple industries and certified for use in federal and state government facilities.

Trellix's Advanced Threat Research team uncovered 4 unique 0-day vulnerabilities and 4 additional undisclosed vulnerabilities leading to remote, unauthenticated code execution on multiple HID Mercury access control panels. These findings lead to full system control including the ability for an attacker to remotely manipulate door locks. During this

presentation, we will briefly cover the hardware debugging process, leading to a root shell on the target. We will explore in greater depth the vulnerability discovery techniques, including emulation, fuzzing, static and dynamic reverse engineering, and a detailed walkthrough of several of the most critical vulnerabilities. We'll address our approach to exploitation using simplistic malware we designed to control system functionality and culminate the talk with a live demo featuring full system control, unlocking doors remotely without triggering any software notification

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## DC - Friday - 14:00-14:20 PDT

---

**Title:** Phreaking 2.0 - Abusing Microsoft Teams Direct Routing

**When:** Friday, Aug 12, 14:00 - 14:20 PDT

**Where:** Caesars Forum - Alliance 301-309, 321 (Track 4)

**SpeakerBio:** Moritz Abrell , SySS GmbH

Moritz Abrell is an experienced expert in Voice-over-IP and network technologies with a focus on information security.

He works as a senior IT security consultant and penetration tester for the Germany-based pentest company SySS GmbH, where he daily deals with the practical exploitation of vulnerabilities and advises customers on how to fix them.

In addition, he regularly publishes his security research in blog posts or presents it at IT security conferences.

Twitter: [@https://twitter.com/moritz\\_abrell](https://twitter.com/moritz_abrell)

### Description:

Microsoft Teams offers the possibility to integrate your own communication infrastructure, e.g. your own SIP provider for phone services. This requires a Microsoft-certified and -approved Session Border Controller. During the security analysis of this federation, Moritz Abrell identified several vulnerabilities that allow an external, unauthenticated attacker to perform toll fraud.

This talk is a summary of this analysis, the identified security issues and the practical exploitation as well as the manufacturer's capitulation to the final fix of the vulnerabilities.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## CPV - Sunday - 12:45-13:30 PDT

---

**Title:** PII: The Privacy Zombie

**When:** Sunday, Aug 14, 12:45 - 13:30 PDT

**Where:** Flamingo - Vista Ballroom

**SpeakerBio:** Alisha Kloc

Alisha Kloc has worked in the security and privacy industry for over a decade, at companies ranging from aerospace behemoths to tech juggernauts to insurance startups. She has given numerous talks about security and privacy around the US and Europe. She is passionate about data security and user privacy, and believes in combining technology, policy, and culture to ensure consumers are protected from the misuse and abuse of personal data.

### Description:

The concept of PII, or personally identifying information, has guided critical decisions around privacy for years. Companies, governments, and consumers believe that protecting a limited subset of data points is sufficient to protect an individual's privacy. But they're dangerously wrong. This talk explains how the term "PII" died a long time ago, why it still lingers in undeath, and what we can do to protect privacy in the modern data era.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## SOC - Friday - 20:00-21:59 PDT

---

**Title:** Pilots and Hackers Meetup

**When:** Friday, Aug 12, 20:00 - 21:59 PDT

**Where:** Caesars Forum - Caucus & Society Boardrooms

### Description:

Aerospace Village presents....

Buzzing the tower – a Pilot / Hacker meetup

Whether you are a hacker, a pilot, or have an interest in either you are welcome to join us at Buzzing the Tower, a meetup hosted by the Aerospace Village. Come and relax, squawk with others, and try your hand at our DEF CON 30 themed Flight Sim challenge! So please stow your tray table in readiness for landing at the destination favoured by pilots and hackers alike!

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## WS - Saturday - 10:00-13:59 PDT

---

**Title:** Pivoting, Tunneling, and Redirection Master Class

**When:** Saturday, Aug 13, 10:00 - 13:59 PDT

**Where:** Harrah's - Copper

**Speakers:**Barrett Darnell,Wesley Thurner

### SpeakerBio:Barrett Darnell , Principal Security Engineer

Barrett Darnell is a Principal Security Engineer on the Intuit Red Team, a vital part of the organization that protects Intuit and customers from all forms of cybercrime. Intuit is the global technology platform that helps consumers and small businesses overcome their most important financial challenges. Serving more than 100 million customers worldwide with TurboTax, QuickBooks, Mint, Credit Karma and Mailchimp, we believe that everyone should have the opportunity to prosper. We never stop working to find new, innovative ways to make that possible.

Prior to Intuit, Barrett was a Managing Senior Operator at Bishop Fox, a security firm providing professional and managed services to the Fortune 1000, global financial institutions, and high-tech startups. Barrett was a technical lead for the Continuous Attack Surface Testing (CAST) Managed Security Service. Before Bishop Fox, he served as an exploitation operator in the US Department of Defense's most elite computer network exploitation (CNE) unit. As a top-rated military officer, Barrett led an offensive operations team in the US Air Force's premier selectively-manned cyber attack squadron.

### SpeakerBio:Wesley Thurner , Principal Security Engineer

Wesley Thurner is a Principal Security Engineer on the Intuit Red Team, a vital part of the organization that protects Intuit and customers from all forms of cybercrime. Intuit is the global technology platform that helps consumers and small businesses

overcome their most important financial challenges. Serving more than 100 million customers worldwide with TurboTax, QuickBooks, Mint, Credit Karma and Mailchimp, we believe that everyone should have the opportunity to prosper. We never stop working to find new, innovative ways to make that possible.

Prior to Intuit, Wesley served as an exploitation operator in the US Department of Defense's most elite computer network exploitation (CNE) unit. There he led and developed multiple teams across a variety of roles in the US Air Force's premier selectively-manned cyber attack squadron. Wes is also a co-organizer for the Red Team Village, a community driven village bridging the gap between penetration testers and offensive operations.

## Description:

Pivoting, tunneling, and redirection are essential skills that separate the junior and senior operators in the offensive security landscape. This workshop describes various techniques used to creatively route traffic through multiple network segments. Various tools and techniques will be discussed and demonstrated. Attendees will be able to practice these skills in a provided cyber range during and after the workshop. These are essential skills for every pentester, bug bounty hunter, and red team operator. But that's not all! Defenders will learn techniques for detecting these sorts of suspicious traffic in their network.

### Materials

Laptop with wireless network adapter

### Prereq

Must have a laptop with an ssh client, students should have beginner experience with ssh and networking.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## LPV - Saturday - 14:00-14:59 PDT

---

**Title:** Please deposit 30c: A history of payphone locks that lead to one of the most secure locks ever made.

**When:** Saturday, Aug 13, 14:00 - 14:59 PDT

**Where:** Caesars Forum - Summit 203-204, 235

### SpeakerBio:

N thing  
No BIO available

## Description:

We will take a look at patents and lock models from payphones through the years leading up to the WE30C and beyond.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## DL - Saturday - 12:00-13:55 PDT

---

**Title:** PMR - PT & VA Management & Reporting

**When:** Saturday, Aug 13, 12:00 - 13:55 PDT

**Where:** Caesars Forum - Committee Boardroom

**Speakers:** Abdul Alanazi,Musaed Bin Muatred

### SpeakerBio:

Abdul Alenazi is a penetration testing technical manager @SabrySecurity, a founding member of Sabry InfoSec, with nearly 8 years of experience in pen testing. Prior to joining Sabry, he has worked as a Penetration Testing Consultant at Booz Allen

Hamilton, HYAS infoSec, ManTech and other Global & Local Companies. Abdul has completed MSc in Computer Engineering with focus on Applied Network Security & Machine Learning at @UVIC.ca. He has also published academic research on Botnet Detection. In his free time, he enjoys coding and investigating open source security tools. Twitter: @alenazi\_90

### **SpeakerBio:**Musaed Bin Muatred

Musaed Bin Muatred: is a Threat Intelligence expert with +8 years of experience in the field of cyber defence. He holds more than 10 certifications and MSc in Computer Science. Also, he has extensive experience in DFIR, threat hunting and reverse engineering

### **Description:**

PMR (PTVA Management & Reporting) is an open-source collaboration platform that closes the gap between InfoSec Technical teams and Management in all assessment phases, from planning to reporting. Technical folks can focus on assessment methodology planning, test execution ,and engagement collaboration. Whereas management can plan engagements, track progress, assign testers, monitor remediation status, and escalate SLA breaches, this is an All-in-One fancy dashboard. The main features are: A) *Asset Management* which allows IT asset inventory tracking with system owner contacts. B) *Engagements Management & Planning* that enable security testers to follow a test execution roadmap by creating a new testing methodology or follow execution standards such as NIST, PTES or OWASP. It definitely will keep pentesting engagements and projects more professional. Also, it enables collaborative testing, gathering information and evidence uploading. C) *Report Automation* that automates boring tasks such as writing technical reports and validation reports. Generating a PDF report that is ready to share with clients and management can be accomplished with one-click. D) *All-in-One Dashboard* that will keep executives and management up-to-date with the organization's security posture. The dashboard components are: - High level of current vulnerabilities. - Engagement progress. - Remediation Status. - Track SLA breaches. -Monitoring risk exceptions.

Audience: Security professionals, Vulnerability Analysts , AppSec, Offense, Risk Management

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

### **CPV - Friday - 11:00-11:30 PDT**

---

**Title:** Positive Identification of Least Significant Bit Image Steganography

**When:** Friday, Aug 12, 11:00 - 11:30 PDT

**Where:** Flamingo - Vista Ballroom

### **SpeakerBio:**Michael Pelosi

Michael Pelosi is associate professor of computer science at Texas A&M University Texarkana. His research publications include artificial intelligence, computer security, steganography and counter-steganography applications.

### **Description:**

Steganography has long been used to counter forensic investigation. This use of steganography as an anti-forensics technique is becoming more widespread. This requires forensic examiners to have additional tools to more effectively detect steganography. In this talk we introduce a new software concept specifically designed to allow the digital forensics professional to clearly identify and attribute instances of least significant bit (LSB) image steganography by using the original cover image in side-by-side comparison with a suspected steganographic payload image. This technique is embodied in a software implementation named CounterSteg.

The CounterSteg software allows detailed analysis and comparison of both the original cover image and any modified image, using sophisticated bit- and color-channel visual depiction graphics. In certain cases, the steganographic software used for message transmission can be identified by the forensic analysis of LSB and other changes in the payload image. This paper demonstrates usage and typical forensic analysis with eight commonly available steganographic programs.

Future work will attempt to automate the typical types of analysis and detection. This is important, as currently there is a steep rise in the use of image LSB steganographic techniques to hide the payload code used by malware and viruses, and for the purposes of data exfiltration. This results because of the fact that the hidden code and/or data can more easily bypass virus and malware signature detection in such a manner as being surreptitiously hidden in an otherwise innocuous image file.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## BTV - Friday - 11:00-12:30 PDT

---

**Title:** Practical Dark Web Hunting using Automated Scripts

**When:** Friday, Aug 12, 11:00 - 12:30 PDT

**Where:** Virtual - BlueTeam Village - Workshops

**SpeakerBio:** Apurv Singh Gautam

Apurv Singh Gautam works as a Threat Researcher at Cyble. He commenced work in Threat Intel 3 years ago. He works on hunting threats from the surface and dark web by utilizing OSINT, SOCMINT, and HUMINT. He is passionate about giving back to the community and has already conducted several talks and seminars at conferences like SANS, Defcon, BSides, local security meetups, schools, and colleges. He loves volunteering with Station X to help students make their way in Cybersecurity. He looks forward to the end of the day to play and stream one of the AAA games Rainbow Six Siege.

### Description:

The workshop will start by taking everyone over why we should focus on the dark web for research and why it is important to collect data from the dark web. We will explore the importance of data collection with some examples. The second part of the workshop will cover some dark web OSINT tools that one can use to start with dark web data collection/hunting. Attendees will learn how these tools work and what different categories of these dark web OSINT tools one can utilize in their research. The third part of the workshop will cover tools and libraries to create your dark web hunting platform. We will explore writing code and automating dark web data collection. This part includes a live lab demo and code explanation. The workshop will end with a few tips on OpSec practices and resources to start with dark web hunting.

Takeaways from the workshop:

1. Understanding why darkerb research is important
2. Darkweb OSINT tools collection to start your research
3. Basic understanding of automated dark web data hunting
4. Python Codebase to start with your dark web data collection

How can you effectively hunt data from the dark web using scripts? How can you circumvent scraping defenses on the dark web? If you are curious about the answers to these questions and want to learn how to effectively write automated scripts for this task, then this workshop is for you. In this workshop, you will learn why collecting data from the dark web is essential, how you can create your tools & scripts, and automate your scripts for effective collection. The workshop's primary focus will be on circumventing defenses put by forums on the dark web against scraping.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## PT - Tuesday - 09:00-16:59 PDT

---

**Title:** Practical Secure Code Review

**When:** Tuesday, Aug 16, 09:00 - 16:59 PDT

**Where:** Caesars Forum

**Speakers:**Seth Law,Ken Johnson

### **SpeakerBio:**Seth Law

Seth Law is an experienced Application Security Professional with over 15 years of experience in the computer security industry. During this time, Seth has worked within multiple disciplines in the security field, from software development to network protection, both as a manager and individual contributor. Seth has honed his application security skills using offensive and defensive techniques, including tool development. Seth is employed as a security consultant, hosts the Absolute AppSec podcast with Ken Johnson, and is a regular speaker at developer meetups and security events, including Blackhat, Defcon, CactusCon, and other regional conferences.

Twitter: [@https://twitter.com/sethlaw](https://twitter.com/sethlaw)

### **SpeakerBio:**Ken Johnson

Ken Johnson, has been hacking web applications professionally for 12 years and given security training for 9 of those years. Ken is both a breaker and builder and currently works on the GitHub application security team. Previously, Ken has spoken at RSA, You Sh0t the Sheriff, Insomnihack, CERN, DerbyCon, AppSec USA, AppSec DC, AppSec California, DevOpsDays DC, LASCON, RubyNation, and numerous Ruby, OWASP, and AWS events about appsec, devops security, and AWS security. Ken's current projects are WeirdAAL, OWASP Railsgoat, and the Absolute AppSec podcast with Seth Law.

Twitter: [@https://twitter.com/cktricky](https://twitter.com/cktricky)

### **Description:**

Latest details, requirements, description, cost:

<https://defcontrainings.myshopify.com/products/seth-law-ken-johnson-practical-secure-code-review>

Training description:

Ready to take your bug hunting to a deeper level? Ever been tasked with reviewing source code for SQL Injection, XSS, Access Control and other security flaws? Does the idea of reviewing code leave you with heartburn? This course introduces a proven methodology and framework for performing a secure code review, as well as addressing common challenges in modern secure code review. Short circuit your development of a custom secure code review process by gleaning from Seth & Ken's past adventures in performing hundreds of code reviews and the lessons we've learned along the way. We will share a proven methodology to perform security analysis of any source code repository and suss out security flaws, no matter the size of the code base, or the framework, or the language.

---

[Return to Index](#) - Add to



- ics [Calendar](#) file

---

## **PT - Monday - 09:00-16:59 PDT**

---

**Title:** Practical Secure Code Review

**When:** Monday, Aug 15, 09:00 - 16:59 PDT

**Where:** Caesars Forum

**Speakers:**Seth Law,Ken Johnson

### **SpeakerBio:**Seth Law

Seth Law is an experienced Application Security Professional with over 15 years of experience in the computer security industry. During this time, Seth has worked within multiple disciplines in the security field, from software development to network protection, both as a manager and individual contributor. Seth has honed his application security skills using offensive and defensive techniques, including tool development. Seth is employed as a security consultant, hosts the Absolute AppSec podcast with Ken Johnson, and is a regular speaker at developer meetups and security events, including Blackhat, Defcon, CactusCon, and other regional conferences.

Twitter: [@https://twitter.com/sethlaw](https://twitter.com/sethlaw)

## **SpeakerBio:**Ken Johnson

Ken Johnson, has been hacking web applications professionally for 12 years and given security training for 9 of those years. Ken is both a breaker and builder and currently works on the GitHub application security team. Previously, Ken has spoken at RSA, You Sh0t the Sheriff, Insomnihack, CERN, DerbyCon, AppSec USA, AppSec DC, AppSec California, DevOpsDays DC, LASCON, RubyNation, and numerous Ruby, OWASP, and AWS events about appsec, devops security, and AWS security. Ken's current projects are WeirdAAL, OWASP Railsgoat, and the Absolute AppSec podcast with Seth Law.

Twitter: [@https://twitter.com/cktricky](https://twitter.com/cktricky)

## **Description:**

Latest details, requirements, description, cost:

<https://defcontrainings.myshopify.com/products/seth-law-ken-johnson-practical-secure-code-review>

Training description:

Ready to take your bug hunting to a deeper level? Ever been tasked with reviewing source code for SQL Injection, XSS, Access Control and other security flaws? Does the idea of reviewing code leave you with heartburn? This course introduces a proven methodology and framework for performing a secure code review, as well as addressing common challenges in modern secure code review. Short circuit your development of a custom secure code review process by gleaning from Seth & Ken's past adventures in performing hundreds of code reviews and the lessons we've learned along the way. We will share a proven methodology to perform security analysis of any source code repository and suss out security flaws, no matter the size of the code base, or the framework, or the language.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## **PT - Tuesday - 09:00-16:59 PDT**

---

**Title:** Pragmatic API Exploration

**When:** Tuesday, Aug 16, 09:00 - 16:59 PDT

**Where:** Caesars Forum

**Speakers:**Aubrey Labuschagne (William),Marianka Botes

## **SpeakerBio:**Aubrey Labuschagne (William)

Aubrey is a security analyst at SensePost. Over the years he has had many roles which included project management, product management, development, training and being a security analyst. Interest for security grew from emergence into information warfare. His hobbies include the development of sensor centric platforms. He has a big passion for training and has completed his masters on how to improve the effectiveness of security awareness programs. He currently holds several certifications which include OSCP, ECSA and ISO 27032 certifications.

Twitter: [@https://twitter.com/cyber\\_protect](https://twitter.com/cyber_protect)

## **SpeakerBio:**Marianka Botes

Marianka is a security analyst for the SensePost team at Orange Cyberdefense. She studied Information Technology at the North-West University (Pukke) in South Africa and has a big passion for hacking. In her off time she will study up some Dad jokes or find the best places to order chicken wings.

Twitter: [@https://twitter.com/mariankabotes](https://twitter.com/mariankabotes)

## **Description:**

Latest details, requirements, description, cost:

<https://defcontrainings.myshopify.com/products/aubrey-labuschagne-william-marianka-botes-pragmatic-api-exploration>

Training description:

The use of Application Programming Interfaces (APIs) have become ubiquitous as business expose and consume services.

Therefore, the threat landscape of organizations increases with the adoption of APIs. The content of the course creates awareness around the various attack vectors used targeting APIs and provides actionable mitigation strategies.

The aim of this course is to empower you to conduct a risk assessment of an API. This hands-on course covers API basics, setting up a test environment, API threat model, API protocols and architectures, typical vulnerabilities, enumerating an attack surface and best practices around security.

Moreover, it focuses on gaining practical experience of the OWASP Top 10 for APIs. In addition, you would be gaining practical experience on exploiting typical vulnerabilities on RESTful (REST) APIs and GraphQL. The course concludes with a capture the flag (CTF) to apply knowledge gained during the course.

---

[Return to Index](#) - Add to



- ics [Calendar](#) file

---

## PT - Monday - 09:00-16:59 PDT

---

**Title:** Pragmatic API Exploration

**When:** Monday, Aug 15, 09:00 - 16:59 PDT

**Where:** Caesars Forum

**Speakers:**Aubrey Labuschagne (William),Marianka Botes

**SpeakerBio:**Aubrey Labuschagne (William)

Aubrey is a security analyst at SensePost. Over the years he has had many roles which included project management, product management, development, training and being a security analyst. Interest for security grew from emergence into information warfare. His hobbies include the development of sensor centric platforms. He has a big passion for training and has completed his masters on how to improve the effectiveness of security awareness programs. He currently holds several certifications which include OSCP, ECSA and ISO 27032 certifications.

Twitter: [@https://twitter.com/cyber\\_protect](https://twitter.com/cyber_protect)

**SpeakerBio:**Marianka Botes

Marianka is a security analyst for the SensePost team at Orange Cyberdefense. She studied Information Technology at the North-West University (Pukke) in South Africa and has a big passion for hacking. In her off time she will study up some Dad jokes or find the best places to order chicken wings.

Twitter: [@https://twitter.com/mariankabotes](https://twitter.com/mariankabotes)

### Description:

Latest details, requirements, description, cost:

<https://defcontrainings.myshopify.com/products/aubrey-labuschagne-william-marianka-botes-pragmatic-api-exploration>

Training description:

The use of Application Programming Interfaces (APIs) have become ubiquitous as business expose and consume services.

Therefore, the threat landscape of organizations increases with the adoption of APIs. The content of the course creates awareness around the various attack vectors used targeting APIs and provides actionable mitigation strategies.

The aim of this course is to empower you to conduct a risk assessment of an API. This hands-on course covers API basics, setting up a test environment, API threat model, API protocols and architectures, typical vulnerabilities, enumerating an attack

surface and best practices around security.

Moreover, it focuses on gaining practical experience of the OWASP Top 10 for APIs. In addition, you would be gaining practical experience on exploiting typical vulnerabilities on RESTful (REST) APIs and GraphQL. The course concludes with a capture the flag (CTF) to apply knowledge gained during the course.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## DC - Sunday - 12:00-12:45 PDT

---

**Title:** PreAuth RCE Chains on an MDM: KACE SMA

**When:** Sunday, Aug 14, 12:00 - 12:45 PDT

**Where:** Caesars Forum - Academy 401-410, 421 (Track 3)

**SpeakerBio:** Jeffrey Hofmann , Security Engineer at Nuro

Jeffrey Hofmann is a Security Engineer at Nuro who loves to do security research both on and off the clock. He has a background in penetration testing and a passion for exploit development/reverse engineering.

Twitter: <https://twitter.com/jeffssh>

### Description:

MDM solutions are, by design, a single point of failure for organizations. MDM appliances often have the ability to execute commands on most of the devices in an organization and provide an “instant win” target for attackers. KACE Systems Management Appliance is a popular MDM choice for hybrid environments. This talk will cover the technical details of 3 preauthentication RCE as root chains on KACE SMA and the research steps taken to identify the individual vulnerabilities used.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## HHV - Saturday - 16:00-16:30 PDT

---

**Title:** Prizes announced for HHV Rube Goldberg Machine, Make Your Own Use Contest, and Bring the Other Half

**When:** Saturday, Aug 13, 16:00 - 16:30 PDT

**Where:** Flamingo - Exec Conf Ctr - Red Rock VI, VII, VII

### Description:

Prizes to be given out for these different events. For more information see - <https://dchhv.org>

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## DC - Friday - 14:00-14:45 PDT

---

**Title:** Process injection: breaking all macOS security layers with a single vulnerability

**When:** Friday, Aug 12, 14:00 - 14:45 PDT

**Where:** Caesars Forum - Academy 401-410, 421 (Track 3)

## **SpeakerBio:** Thijs Alkemade , Security Researcher at Computest

Thijs Alkemade (@xnyhps) works at the security research division of at Computest. This division is responsible for advanced security research on commonly used systems and environments. Thijs has won Pwn2Own twice, by demonstrating a zero-day attack against Zoom at Pwn2Own Vancouver 2021 and by demonstrating multiple exploits in ICS systems at Pwn2Own Miami 2022. In previous research he demonstrated several attacks against the macOS and iOS operating systems. He has a background in both mathematics and computer science, which gives him a lot of experience with cryptography and programming language theory.

Twitter: [@https://twitter.com/xnyhps](https://twitter.com/xnyhps)

## **Description:**

macOS local security is shifting more and more to the iOS model, where every application is codesigned, sandboxed and needs to ask for permission to access sensitive data. New security layers have been added to make it harder for malware that has gained a foothold to compromise the user's most sensitive data. Changing the security model of something as large and established as macOS is a long process, as it requires many existing parts of the system to be re-examined. For example, creating a security boundary between applications running as the same user is a large change from the previous security model.

CVE-2021-30873 is a process injection vulnerability we reported to Apple that affected all macOS applications. This was addressed in the macOS Monterey update, but completely fixing this vulnerability requires changes to all third-party applications as well. Apple has even changed the template for new applications in Xcode to assist developers with this.

In this talk, we'll explain what a process injection vulnerability is and why it can have critical impact on macOS. Then, we'll explain the details of this vulnerability, including how to exploit insecure deserialization in macOS. Finally, we will explain how we exploited it to escape the macOS sandbox, elevate our privileges to root and bypass SIP.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## **BTW - Sunday - 12:00-12:59 PDT**

---

**Title:** Project Obsidian: Panel Discussion

**When:** Sunday, Aug 14, 12:00 - 12:59 PDT

**Where:** Flamingo - Savoy Ballroom - BTW Main Stage

## **Description:**

- How was Project Obsidian put together
- Involved a global village
- Opportunities for mentoring
- Look behind the scenes of a CTF
- and more

Blue Team Village's Project Obsidian is an immersive, defensive cybersecurity learning experience that provides attendees with the opportunity to gain knowledge of Incident Response (IR), Digital Forensics (DF), Reverse Engineering Malware (REM), Cyber Threat Intelligence (CTI), and Cyber Threat Hunting (CTH).

Project Obsidian crew members talk about how they put it all together.

Blue Team Village's Project Obsidian is an immersive, defensive cybersecurity learning experience that provides attendees with the opportunity to gain knowledge of Incident Response (IR), Digital Forensics (DF), Reverse Engineering Malware (REM), Cyber Threat Intelligence (CTI), and Cyber Threat Hunting (CTH).

## PLV - Sunday - 12:00-13:45 PDT

---

**Title:** Protect Our Pентest Tools! Perks and Hurdles in Distributing Red Team Tools

**When:** Sunday, Aug 14, 12:00 - 13:45 PDT

**Where:** Caesars Forum - Summit 226-227 - Policy Roundtable

### Description:

A panel with Q&A about offensive cybersecurity tools like CobaltStrike, how the tools affect both defensive and offensive security practitioners, and the practical difficulties of controlling the licenses and distribution of these pentest tools. This is meant to be an impact-focused discussion on the merits and challenges of producing offensive tools and NOT a law-based debate/interpretation of export controls.

---

## WS - Thursday - 10:00-13:59 PDT

---

**Title:** Protect/hunt/respond with Fleet and osquery

**When:** Thursday, Aug 11, 10:00 - 13:59 PDT

**Where:** Harrah's - Goldfield + Tonopah

**Speakers:**Guillaume Ross,Kathy Satterlee

### SpeakerBio:Guillaume Ross , Head of Security

Guillaume started hacking away in the early 90s. Whereby hacking, we mean "understanding how pkzip works so he could fit this game on his ridiculous HDD". He then went on to work in IT, focusing on large scale endpoint deployments for a few years. He then became a security consultant, working with all types of different organizations, doing endpoint security, mobile security, and cloud security until he started leading security in startups. Guillaume is currently the Head of Security at Fleet Device Management, the company behind the open source project Fleet. Guillaume dislikes doing meaningless "best practices" work that has no practical value and enjoys leveraging great open source software available to all of us to improve security.

Guillaume has spoken and given workshops at various conferences like BSidesLV, BsidesSF, DEF CON, RSAC, Thotcon and Northsec on many topics, including mobile security, endpoint security, logging and monitoring.

### SpeakerBio:Kathy Satterlee , Developer Advocate

Kathy is a Developer Advocate at Fleet Device Management. She generally has a pretty good idea of how Fleet and osquery work together and what people are doing with them. She also usually knows who to reach out to when she doesn't have a clue.

### Description:

In this workshop, we will learn how to use Fleet and osquery to ensure systems are protected, detect suspicious activity, hunt for attackers, and respond to incidents. First, we'll see how to deploy Fleet to manage osquery agents. Then, we will use shared Fleet instances to track the security posture of systems, inventory vulnerable applications, and perform threat hunting. These Fleet instances will be connected to a shared Slack workspace, where we will generate custom alerts to ensure insecure systems can be dealt with. These shared Fleet instances will output data to centralized logging (Graylog), which we will use to create dashboards as well as alerting for suspicious activity. At the end of this workshop, you'll know how to use Fleet and osquery to ensure your workstations and servers are secure, to quickly find vulnerable systems as well as discover attackers

performing techniques such as establishing persistence and privilege escalation.

## Materials

A laptop with internet access, a web browser, virtualization app such as VirtualBox or VMware, and Docker (on main OS or in a VM). We recommend bringing at least one or two VMs (Mac, Windows or Linux) ready to use as osquery clients.

## Prereq

Basic understanding of operating systems and networking. No knowledge of Fleet or osquery itself is needed.

---

[Return to Index](#) - Add to



- ics [Calendar file](#)

---

## CLV - Friday - 15:00-16:59 PDT

---

**Title:** Prowler Open Source Cloud Security: A Deep Dive Workshop

**When:** Friday, Aug 12, 15:00 - 16:59 PDT

**Where:** Flamingo - Scenic Ballroom

**SpeakerBio:** Toni de la Fuente

No BIO available

Twitter: [@https://twitter.com/ToniBlyx](https://twitter.com/ToniBlyx)



## Description:

Whether you are a long time Prowler user or if you are just getting started, this workshop will give you the tools to get AWS security up and running and under control at your organization. With millions of downloads and a large community of users, Prowler is one of the most used tools when it comes to AWS security assessments, hardening, incident response and security posture monitoring. Prowler has some new features and important changes coming in v3.0. This includes a new check architecture, python support, and a load of new checks for compliance and AWS services. In addition to allowing us to build new checks with the existing bash/aws-cli support we will teach how to do it with python as well and going beyond the AWS API and increasing the coverage of Prowler to get the most of it and adapt it to your requirements.

---

[Return to Index](#) - Add to



- ics [Calendar file](#)

---

## CPV - Friday - 12:00-12:30 PDT

---

**Title:** PSA: Doorbell Cameras Have Mics, Too

**When:** Friday, Aug 12, 12:00 - 12:30 PDT

**Where:** Flamingo - Vista Ballroom

**Speakers:** Yael Grauer, Matthew Guariglia

**SpeakerBio:** Yael Grauer

Yael Grauer is an investigative tech reporter covering privacy and security at Consumer Reports. She manages Security Planner, a free, easy-to-use guide to staying safer online.

**SpeakerBio:** Matthew Guariglia

Dr. Matthew Guariglia is a historian of policing and surveillance and a policy analyst at EFF, where he works on issues of surveillance at the local, state, and federal level.

## Description:

Millions of video doorbells have been installed outside of U.S. homes. They're so ubiquitous that you might expect to be captured on other people's video feeds every time you walk or drive down the street. What you might not be aware of is that video doorbells can record audio, too. Conversations you have in your own home or when walking by a neighbor's house may be sitting on Amazon's servers. You might be recording audio from unsuspecting passersby, too. In this talk, we'll discuss new Consumer Reports research—both in our lab and outside of our smart home reporter's home—on audio capture distance. We'll delve into potential risks and privacy concerns. And we'll discuss what video doorbell owners can do (short of getting rid of the devices altogether).

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## DC - Friday - 18:00-18:45 PDT

---

**Title:** Pulling Passwords out of Configuration Manager: Practical Attacks against Microsoft's Endpoint Management Software

**When:** Friday, Aug 12, 18:00 - 18:45 PDT

**Where:** Caesars Forum - Academy 401-410, 421 (Track 3)

**SpeakerBio:** Christopher Panayi , Chief Research Officer, MWR CyberSec

Christopher is the Chief Research Officer at MWR CyberSec (<https://mwrcybersec.com>), having previously led cyber-defense, red team, and targeted attack simulation (TAS) engagements for several years, as well as having designed and helped run the in-house training programme for security consultants at MWR. As part of this work, a major focus area for him had been understanding attack techniques impacting Active Directory (AD); this led to publications such as: a discussion of practical ways to perform pass-the-hash attacks (<https://labs.f-secure.com/blog/pth-attacks-against-ntlm-authenticated-web-applications/>) and a discussion of the previous gold standard in AD security, the red forest, and why it did not meet its goal of making environments more secure in many cases (<https://www.f-secure.com/content/dam/press/ja/media-library/reports/F-Secure%20Whitepaper%20-%20Tending%20To%20the%20Red%20Forest.pdf>). His interest in how things work at a deep technical level - and desire to develop an understanding of how to use this information to compromise and secure systems and environments - has led him to his current focus, investigating and understanding Microsoft Endpoint Configuration Manager, how it interacts with AD, and how to abuse its configuration to attack enterprise environments.

Twitter: [@https://twitter.com/Raiona\\_ZA](https://twitter.com/Raiona_ZA)

## Description:

System Center Configuration Manager, now Microsoft Endpoint Configuration Manager (MECM), is a software management product that has been widely adopted by large organizations to deploy, update, and manage software; it is commonly responsible for the deployment and management of the majority of server and workstation machines in enterprise Windows environments.

This talk will provide an outline of how MECM is used to deploy machines into enterprise environments (typically through network booting, although it supports various Operating System deployment techniques), and will explore attacks that allow Active Directory credentials to be extracted from this process. The common MECM misconfigurations leading to these attacks will be detailed and, in so doing, the talk will aim to show how to identify and exploit these misconfigurations and how to defend against these attacks. Each viable attack will be discussed in depth (mostly by discussing the protocols and architecture in use, but sometimes by diving into relevant code, if necessary) so that the context of how and why the attack works will be understood. These concepts will be illustrated through the demo and release of a tool that allows for the extraction of credentials from several of the onsite deployment techniques that MECM supports.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

**Title:** Purple Teaming & Adversary Emulation in the Cloud with Stratus Red Team

**When:** Saturday, Aug 13, 11:20 - 11:59 PDT

**Where:** Flamingo - Scenic Ballroom

**SpeakerBio:** Christophe Tafani-Dereeper

Christophe is a cloud security researcher and advocate at Datadog. He's passionate about threat detection in the cloud, and cloud-native technologies in general. He previously worked as a software developer, penetration tester, SOC analyst and cloud security engineer. He likes to write about technology he likes, uses, dislikes and misuses. Living in Switzerland, you can tell he's French when he speaks.

Twitter: <https://twitter.com/christophetd>

### Description:

To detect evil in the cloud, you must first know what 'evil' looks like. Then, it's critical to have an easy way to reproduce common attack techniques in live environments, to validate that our threat detection and logging pipelines work as intended. In this talk, we present Stratus Red Team, an open-source project for adversary emulation and end-to-end validation of threat detection in AWS, Kubernetes and Azure.

We discuss the motivation behind the project, design choices, and the philosophy behind Stratus Red Team: helping blue teams focus on real-world, documented attack techniques and empower them to iteratively build high-quality detections. We also discuss more advanced use-cases that Stratus Red Team allows, such as running it on a schedule in your CI/CD to continuously validate that the expected alerts are popping up in your SIEM.

We conclude with a live demo where we 'detonate' attack techniques against a live Kubernetes cluster and AWS account.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## CPV - Saturday - 17:00-17:59 PDT

---

**Title:** Pursuing Phone Privacy Protection [WORKSHOP]

**When:** Saturday, Aug 13, 17:00 - 17:59 PDT

**Where:** Flamingo - Vista Ballroom

**Speakers:** Mauricio Tavares, Matt Nash

**SpeakerBio:** Mauricio Tavares

Mauricio Tavares confuses people and things

Mauricio has worked in both the private industry -- credit card and medical -- and multinational research projects, which led to an interest in the behavioral aspect of data security and privacy. He has published in topics ranging from aerospace engineering to computer automation and data privacy (or lack of thereof). Currently, he helps organizations understand the importance of protecting their bacon, including tasty user and data privacy, using expressive dancing.

He only knows two facts about geese, both of which are wrong.

**SpeakerBio:** Matt Nash

Matt Nash breaks things (sometimes intentionally)

As a security consultant, Matt works in a variety of realms, including: internal/external network infrastructure, cloud environments, web applications, automated teller machines (ATMs), physical security, social engineering, digital forensics and incident response, mobile, and wireless. As well, these assessments span a number of sectors: energy, utility, manufacturing, software development, financial, retail, municipal, and medical.

Matt holds a B.S. in Food and Resource Economics, and as a result is totally qualified to speak on the topic being discussed today.

## Description:

New year, new challenges to privacy.

You are in a public event, or a coffee shop. Did a notification just tell you about a sale nearby? Why is this app showing ads for the car you rented and told your friend about? Is Santa Claus the only one who knows if you've been naughty or nice? "Maybe if I run a VPN I will be safe." This is wishful thinking at best; it only helps to deal with some privacy attacks. You see, smart phones are little snitches. By design.

They listen to you. They know where you go, what you purchase, and who you interact with. And they never sleep or take vacations.

You can fight back. You can regain (at least some) control of your privacy! But it will not be done buying some magic software and pressing the EZ button. Some assembly is required.

If you are willing to roll up your sleeves and take your brave pill, join us in this workshop as we show how to build your Android phone with the balance between privacy, security, and convenience that fits your comfort level.

Attendees will come out of this workshop with a privacy mindset:

Appreciating the privacy and security implications of using a smart phone in general -- specifically consumer Android devices. Knowing how to achieve different levels of privacy in their phones and understanding the costs and benefits of each approach. Understanding what "attribution of traffic" tying IP to a person through a VPN is. Finding out which apps are privacy-respecting, and how to contain untrusted apps that may be a "must have".

[Who should take this workshop]

Privacy-conscious smartphone users who would like to understand and control what their phones share about them.

[Audience Skill Level]

Intermediate

Entry level, if you have studied the instructions and are prepared to hit the ground running. Or if your team is willing to help you out. We will NOT be able to wait for you to install 374 OS updates, download and install VirtualBox, and then build a Linux VM.

[Attendees' requirements]

An understanding of basic Linux commands. Be comfortable with the idea of installing an aftermarket firmware/OS ("ROM") on a mobile device. Soft/hard "bricking" is a possibility, so having a spare phone may be a good investment. Follow additional instructions provided on the GitHub repository (<https://github.com/matthewnash/building-phone-privacy/wiki>) ahead of the workshop.

[What students should bring (or do beforehand)]

An Android phone that has been configured per the GitHub instructions. Alternatively, a laptop with Android Studio installed. A learning attitude.

## ASV - Saturday - 10:30-10:55 PDT

---

**Title:** Quantum Snake Oil? What Ailments Can It Cure?

**When:** Saturday, Aug 13, 10:30 - 10:55 PDT

**Where:** Caesars Forum - Forum 112-117

**SpeakerBio:** Jose Pizarro , System Engineer

Jose Pizarro is System Engineer at ESA covering over 20 years of experience. He's pulled cables under the floors of various labs covering space robotics to quantum communications

### Description:

This presentation will provide a short primer on Quantum Communications in the Aerospace (Communications, Computing and Cybersecurity). We will cover what Quantum Communications overpromises (It will make you coffee in the morning) & talk about the right tools for the right job. Finally, an overview of the engineering challenges to implementing a QKD system in space will also be discussed.

---

## SOC - Saturday - 16:00-17:59 PDT

---

**Title:** Queercon Mixer

**When:** Saturday, Aug 13, 16:00 - 17:59 PDT

**Where:** Caesars Forum - Forum 120-123, 129, 137

### Description:

The lgbtqia+ community in InfoSec is throwing a party to bring our folk together and have a good time. Meet others like you or hang out with those you've met over the years. This is a safe and inclusive space meant to make you feel comfortable and help you socialize with others like you.

---

## SOC - Friday - 16:00-17:59 PDT

---

**Title:** Queercon Mixer

**When:** Friday, Aug 12, 16:00 - 17:59 PDT

**Where:** Caesars Forum - Forum 120-123, 129, 137

### Description:

The lgbtqia+ community in InfoSec is throwing a party to bring our folk together and have a good time. Meet others like you or hang out with those you've met over the years. This is a safe and inclusive space meant to make you feel comfortable and help you socialize with others like you.

---

## SOC - Thursday - 16:00-17:59 PDT

---

**Title:** Queercon Mixer

**When:** Thursday, Aug 11, 16:00 - 17:59 PDT

**Where:** Caesars Forum - Forum 120-123, 129, 137

### Description:

The lgbtqia+ community in InfoSec is throwing a party to bring our folk together and have a good time. Meet others like you or hang out with those you've met over the years. This is a safe and inclusive space meant to make you feel comfortable and help you socialize with others like you.

---

## SOC - Friday - 22:00-00:59 PDT

---

**Title:** Queercon Party

**When:** Friday, Aug 12, 22:00 - 00:59 PDT

**Where:** Caesars Forum - Forum 108-110

### Description:

The lgbtqia+ community in InfoSec is throwing a party to bring our folk together and have a good time. Meet others like you or hang out with those you've met over the years. This is a safe and inclusive space meant to make you feel comfortable and help you socialize with others like you.

---

## BHV - Saturday - 13:30-14:30 PDT

---

**Title:** Radical inclusivity and intersectionality in the biohacking world

**When:** Saturday, Aug 13, 13:30 - 14:30 PDT

**Where:** Flamingo - Laughlin I,II,III

### SpeakerBio:

Berkelly Gonzalez

Berkelly Gonzalez is a biohacker and undergraduate Physics student studying at UC Berkeley who is passionate about issues surrounding healthcare as a human right, bodily autonomy, and accessibility within the scientific community.

### Description:

Cyborgs and mutants are not fictional creatures relegated to the realm of sci-fi and superheroes, they are all around us: regular people with pacemakers and prosthetics, with cancer and chronic illness, as well as gender queer and neurodivergent people. For cyborgs and mutants, biohacking often isn't just a hobby, it is a method of survival. This workshop aims to examine the history, ethics, and legalities of various forms of biohacking and their impact on gender queer, disabled, chronically ill, and neurodivergent persons.

---

## BTV - Friday - 13:00-14:30 PDT

---

**Title:** Ransomware ATT&CK and Defense

**When:** Friday, Aug 12, 13:00 - 14:30 PDT

**Where:** Virtual - BlueTeam Village - Workshops

**Speakers:**Ronny Thammasathiti,Daniel Chen,Esther Matut,Ben Hughes,Nick Baker

### **SpeakerBio:**Ronny Thammasathiti

Ronny Thammasathiti (@ronnyt) started out as an aspiring concert pianist but later took a big switch to cyber security with Polito Inc in the past 4 years. His main role at the company is as a detection Engineer using Elasticsearch and developing tools and applications using his knowledge of Python language.

### **SpeakerBio:**Daniel Chen

DFIR consultant and penetration tester at Polito Inc. I investigated numerous ransomware incidents, hunted for adversaries, and assisted with red teaming.

### **SpeakerBio:**Esther Matut

To be completed.

### **SpeakerBio:**Ben Hughes

Ben Hughes (@CyberPraesidium) brings over 15 years of diverse experience in cybersecurity, IT, and law. He leads Polito Inc.'s commercial cybersecurity services including threat hunting, digital forensics and incident response (DFIR), penetration testing, red teaming, adversary emulation, and training. Prior to Polito, Ben worked on APT hunt teams at federal and commercial clients. He currently holds CISSP, GCFA, GWAPT, and endpoint security vendor certifications.

### **SpeakerBio:**Nick Baker

Nick Baker has over 10 years in cybersecurity. Prior to Polito, Nick spent 20 years as a Signal Warrant Officer in the U.S. Army. He performed over 10 years in the cybersecurity field with a heavy focus in computer network defense by providing expertise for the proper employment, support, and defense of strategic and tactical information networks, systems, and services in operations supporting the Army's cyberspace domain. Nick's other 10 years was providing IT support, operations, and functions. I hold multiple credentials including SANS, CompTIA and ICS2.

### **Description:**

This hands-on training workshop will walk attendees through threat hunting exercises to detect and investigate common Tactics, Techniques, and Procedures (TTPs) frequently used by ransomware threat actors during an attack. From Reconnaissance and Initial Access to Exfiltration and Impact, attendees will be exposed to a compressed ransomware attack lifecycle while being able to leverage attack TTPs including commands, scripts, tools, communication channels, and techniques that we frequently see and use in the wild. Tactics and techniques will be mapped to the MITRE ATT&CK Framework, and will be inspired by ATT&CK's Adversary Emulation Plans. The workshop will accordingly incorporate offensive operation elements such as adversary emulation and red teaming, but with an emphasis on purple teaming and blue teaming. In other words, we will explore the logs and other artifacts potentially left behind by our attack TTPs and how the blue team might utilize endpoint and network logs and defensive tooling to detect and disrupt the ATT&CK kill chain components. Examples of tools and threat intelligence sources that will be incorporated include Atomic Red Team, open-source offensive security tools such as Mimikatz, Living off the Land Binaries and Scripts (LOLBAS) including PowerShell, real-world or Proof-of-Concept malware samples and exploits, and leaked ransomware playbooks supplemented by other open-source intelligence (OSINT) sources; and specifically on the blue team side, popular security logging pipeline and Security Information and Events Management (SIEM) tools such as Sysmon and Elastic Stack.

This hands-on training workshop will walk attendees through hunting for Tactics, Techniques, and Procedures (TTPs) frequently used by ransomware adversaries. From Reconnaissance and Initial Access to Exfiltration and Impact, attendees will be exposed to a compressed ransomware attack lifecycle. Workshop TTPs will be mapped to the MITRE ATT&CK Framework, and it will incorporate offensive operation elements such as adversary emulation, but while emphasizing purple and blue teaming. We will explore the endpoint and network logs left behind by attack TTPs and how the blue team can utilize such logs and defensive tooling to detect and disrupt the attack.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## ASV - Saturday - 10:00-15:59 PDT

---

**Title:** Red Balloon Failsat Challenges

**When:** Saturday, Aug 13, 10:00 - 15:59 PDT

**Where:** Caesars Forum - Forum 112-117

### Description:

Red Balloon Security will provide satellite modems as well as a small satellite for the modems to communicate with. We will provide support and training at the event to help people work through all steps of the challenges using OFRAK. OFRAK (Open Firmware Reverse Analysis Konsole) combines the ability to unpack, analyze, modify, and repack binaries & firmware in a single application. PWNSAT CHALLENGE Participants will analyze and modify the modem firmware with the goal of successfully patching in shellcode to send malicious commands to the CubeSat to make it spin. Modifications may include – disabling firewall, finding credentials, and shellcode writing + injection. Winners with the most interesting CubeSat spin results will be rewarded with a prize.

**SAFE SPACE: SATELLITE CONTROL PATCHING** In this challenge, participants will have the opportunity to construct and apply a patch modeled after a real world bug detected in spacecrafts. The challenge will be to understand and patch code that's trying to solve an equation, but has a bug that makes the satellite unusable. We provide guidance on how to identify the mistake and present multiple approaches in increasing degrees of patching complexity.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## ASV - Friday - 10:00-15:59 PDT

---

**Title:** Red Balloon Failsat Challenges

**When:** Friday, Aug 12, 10:00 - 15:59 PDT

**Where:** Caesars Forum - Forum 112-117

### Description:

Red Balloon Security will provide satellite modems as well as a small satellite for the modems to communicate with. We will provide support and training at the event to help people work through all steps of the challenges using OFRAK. OFRAK (Open Firmware Reverse Analysis Konsole) combines the ability to unpack, analyze, modify, and repack binaries & firmware in a single application. PWNSAT CHALLENGE Participants will analyze and modify the modem firmware with the goal of successfully patching in shellcode to send malicious commands to the CubeSat to make it spin. Modifications may include – disabling firewall, finding credentials, and shellcode writing + injection. Winners with the most interesting CubeSat spin results will be rewarded with a prize.

**SAFE SPACE: SATELLITE CONTROL PATCHING** In this challenge, participants will have the opportunity to construct and apply a patch modeled after a real world bug detected in spacecrafts. The challenge will be to understand and patch code

that's trying to solve an equation, but has a bug that makes the satellite unusable. We provide guidance on how to identify the mistake and present multiple approaches in increasing degrees of patching complexity.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## ASV - Sunday - 10:00-11:59 PDT

---

**Title:** Red Balloon Failsat Challenges

**When:** Sunday, Aug 14, 10:00 - 11:59 PDT

**Where:** Caesars Forum - Forum 112-117

### Description:

Red Balloon Security will provide satellite modems as well as a small satellite for the modems to communicate with. We will provide support and training at the event to help people work through all steps of the challenges using OFRAK. OFRAK (Open Firmware Reverse Analysis Konsole) combines the ability to unpack, analyze, modify, and repack binaries & firmware in a single application. PWNSAT CHALLENGE Participants will analyze and modify the modem firmware with the goal of successfully patching in shellcode to send malicious commands to the CubeSat to make it spin. Modifications may include – disabling firewall, finding credentials, and shellcode writing + injection. Winners with the most interesting CubeSat spin results will be rewarded with a prize.

**SAFE SPACE: SATELLITE CONTROL PATCHING** In this challenge, participants will have the opportunity to construct and apply a patch modeled after a real world bug detected in space crafts. The challenge will be to understand and patch code that's trying to solve an equation, but has a bug that makes the satellite unusable. We provide guidance on how to identify the mistake and present multiple approaches in increasing degrees of patching complexity.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## CPV - Friday - 13:00-13:30 PDT

---

**Title:** Reflections on 9 Years of CPV

**When:** Friday, Aug 12, 13:00 - 13:30 PDT

**Where:** Flamingo - Vista Ballroom

**SpeakerBio:** Whitney Merrill

No BIO available

**Description:** No Description available

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## DL - Saturday - 14:00-15:55 PDT

---

**Title:** ResidueFree

**When:** Saturday, Aug 13, 14:00 - 15:55 PDT

**Where:** Caesars Forum - Committee Boardroom

## **SpeakerBio:** Logan Arkema

Logan is a former student-turned-independent researcher and software developer. While he makes a living conducting IT, security, and privacy audits, his most impactful hacking is 1337ing his job's policies as a union rep to elevate workplace privileges. He has an OSCP, other certs from days wooing federal hiring screeners to pass along his application, and The Time Warp stuck in his head from the time he heard "rm -rf" could be pronounced "rimm raff."

## **Description:**

ResidueFree is a privacy-enhancing tool that allows individuals to keep sensitive information off their device's filesystem. It takes on-device privacy protections from TAILS and "incognito" web browser modes and applies them to any app running on a user's regular operating system, effectively making the privacy protections offered by TAILS more usable and accessible while improving the on-device privacy guarantees made by web browsers and extending them to any application. While ResidueFree currently runs on Linux, its maintainers are hoping to port it to other operating systems in the near future. In addition, ResidueFree can help forensic analysts and application security engineers isolate filesystem changes made by a specific application. The same implementation ResidueFree uses to ensure that any file changes an application makes are not stored to disk can also be used to isolate those changes to a separate folder without impacting the original files.

**Audience:** ResidueFree was primarily developed for individuals facing privacy threats that can access the information stored on the individuals' device. However, this presentation is also designed for security trainers that want to expand the tools they can suggest as well as for privacy engineers interested in contributing to ResidueFree or expanding it to more commonly used operating systems. ResidueFree also has features built for malware or forensic analysts, application security engineers, or others who wish to easily isolate an application's changes to a device's filesystem with a simple tool.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## **ASV - Friday - 13:00-14:59 PDT**

---

**Title:** Resumé Review and Career Guidance Session

**When:** Friday, Aug 12, 13:00 - 14:59 PDT

**Where:** Caesars Forum - Forum 112-117

## **Description:**

Bring yourself and a copy of your resume to discuss your career trajectory with public and private industry leaders. Prepare your questions or sit in a mock interview as you hone your skills for a future in aerospace cybersecurity.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## **ASV - Saturday - 13:00-14:59 PDT**

---

**Title:** Resumé Review and Career Guidance Session

**When:** Saturday, Aug 13, 13:00 - 14:59 PDT

**Where:** Caesars Forum - Forum 112-117

## **Description:**

Bring yourself and a copy of your resume to discuss your career trajectory with public and private industry leaders. Prepare your questions or sit in a mock interview as you hone your skills for a future in aerospace cybersecurity.

## PLV - Saturday - 14:00-15:45 PDT

---

**Title:** Return-Oriented Policy Making for Open Source and Software Security

**When:** Saturday, Aug 13, 14:00 - 15:45 PDT

**Where:** Caesars Forum - Summit 226-227 - Policy Roundtable

**Speakers:**Trey Herr,Eric Mill,Harry Mourtos,Jack Cable

**SpeakerBio:**Trey Herr , Director

Trey Herr is the director of the Cyber Statecraft Initiative under the Scowcroft Center for Strategy and Security at the Atlantic Council. His team works on cybersecurity and geopolitics including cloud computing, the security of the internet, supply chain policy, cyber effects on the battlefield, and growing a more capable cybersecurity policy workforce. Previously, he was a senior security strategist with Microsoft handling cloud computing and supply chain security policy as well as a fellow with the Belfer Cybersecurity Project at Harvard Kennedy School and a non-resident fellow with the Hoover Institution at Stanford University. He holds a PhD in Political Science and BS in Musical Theatre and Political Science.

**SpeakerBio:**Eric Mill , US Office of Management and Budget

No BIO available

**SpeakerBio:**Harry Mourtos , Office of the National Cyber Director

No BIO available

**SpeakerBio:**Jack Cable , Congressional Fellow, Senate Homeland Security and Government Accountability Committee

No BIO available

### Description:

A moderated discussion on how to hack policy systems using laws and authorities already on the books, featuring the policymakers who write and use them, focusing on open source and software security. At DefCon 22 in the aftermath of Heartbleed, John Menerick told us to "keep calm and hide the internet". Alas, they found it. The policy community in the US, and lesser extent Europe, is finally starting to put serious focus on software security including open source. This event will bring hackers together with policymakers to identify policies on the book that could help improve the open source ecosystem and the security of software. Other policy conversations might stray into the possible, this one will emphasize the practical. The discussion will involve policymakers who write and implement these laws and use these authorities to enable discussion and debate focused on pragmatic solutions, putting hackers inside ongoing policy debates in real time.

---

## HHV - Friday - 13:00-13:45 PDT

---

**Title:** Reversing An M32C Firmware – Lesson Learned From Playing With An Uncommon Architecture

**When:** Friday, Aug 12, 13:00 - 13:45 PDT

**Where:** Flamingo - Exec Conf Ctr - Red Rock VI, VII, VII

**SpeakerBio:**Philippe Laulheret

Philippe Laulheret is a Senior Security Researcher on the Trellix vulnerability research team. With a focus on Reverse Engineering and Vulnerability Research, Philippe uses his background in Embedded Security and Software Engineering to

poke at complex systems and get them behave in interesting ways. In his spare time, Philippe enjoys playing CTFs, immersing himself in the beauty of the Pacific Northwest, and exploring the realm of Creative Coding.

Philippe holds a MSc in Computer Science from Georgia Tech and a MSc in Electrical and Computer Engineering from Supélec (France).

### Description:

While busy hacking the planet, have you ever encountered an unfamiliar architecture and simply had no idea where to start? You pried the firmware from a reluctant (and almost not smoldering) flash chip, loaded the thing in IDA, but what's next? We got into this pickle while working on reversing the firmware of a medical device. The mystery architecture turned out to be M32C, and thankfully, IDA Pro added support for it a few months prior.

This talk is not exactly about reversing yet another embedded device. Instead, this is more about the journey and lessons learned so that it could be abstracted away for the next project. Rather than focusing on the specifics of the firmware itself, we will see how it interacts with the micro-controller and the steps taken to approach an unfamiliar embedded architecture.

During this presentation, you can expect digging into low-level micro-controller notions such as interrupt handlers, special purpose registers, how to find flash handling code, and way too much M32C assembly. If you've ever dabbled in hardware hacking and want to have a look at something that is not Linux-based, this talk will give you some pointers in how to get the ball *rolling*. (not talking about the ones we dropped at the reballing station)

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## DC - Saturday - 11:30-12:15 PDT

---

**Title:** Reversing the Original Xbox Live Protocols

**When:** Saturday, Aug 13, 11:30 - 12:15 PDT

**Where:** Caesars Forum - Forum 104-105, 135-136 (Track 1)

**SpeakerBio:** Tristan Miller , Hacker

monocasa has over a decade of industry experience as an engineer in related sub-fields such as firmware development, binary reversing, cloud based device and identity management, and custom tunneling of IP.

### Description:

Xbox Live for original Xbox systems launched on November 15, 2002 and was subsequently discontinued on April 15, 2010. The first half of this talk will be an information dense overview of the gritty details of how the underlying protocols work and intermixing a retrospective of two decades of how the industry has approached IOT and network security. The second half of the talk will use that base to discuss the architecture of drop in replacement server infrastructure, how the speaker approaches the ethics of third party support for non-updatable abandoned networked devices, and culminating in a demo.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## DC - Sunday - 13:00-13:45 PDT

---

**Title:** RingHopper – Hopping from User-space to God Mode

**When:** Sunday, Aug 14, 13:00 - 13:45 PDT

**Where:** Caesars Forum - Forum 106-110, 138-139 (Track 2)

**Speakers:** Jonathan Lusky, Benny Zeltser

**SpeakerBio:** Jonathan Lusky , Security Research Team Lead, Intel  
No BIO available

**SpeakerBio:** Benny Zeltser , Security Researcher, Intel  
No BIO available

### Description:

The SMM is a well-guarded fortress that holds a treasure – an unlimited god mode. We hopped over the walls, fooled the guards, and entered the holy grail of privileges. An attacker running in System Management Mode (SMM) can bypass practically any security mechanism, steal sensitive information, install a bootkit, or even brick the entire platform. We discovered a family of industry wide TOCTOU vulnerabilities in various UEFI implementations affecting more than 8 major vendors making billions of devices vulnerable to our attack. RingHopper leverages peripheral devices that exist on every platform to perform a confused deputy attack. With RingHopper we hop from ring 3 (user-space) into ring -2 (SMM), bypass all mitigations, and gain arbitrary code execution. In our talk, we will deep-dive into this class of vulnerabilities, exploitation method and how it can be prevented. Finally, we will demonstrate a PoC of a full exploitation using RingHopper, hopping from user-space into SMM.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## HHV - Saturday - 13:00-13:45 PDT

---

**Title:** RoboSumo

**When:** Saturday, Aug 13, 13:00 - 13:45 PDT

**Where:** Flamingo - Exec Conf Ctr - Red Rock VI, VII, VII

### Description:

Bring a robo sumo and compete. Details at - <https://dchhv.org/events/robosumo.html>

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## RHV - Friday - 11:00-11:59 PDT

---

**Title:** Rock the Cash Box

**When:** Friday, Aug 12, 11:00 - 11:59 PDT

**Where:** Caesars Forum - Alliance 310, 320

**SpeakerBio:** Spicy Wasabi

Tinkerer of electronics, radios, and sometimes servers. Perpetual volunteer for many events including CCDC, CPTC, and a few conferences.

Twitter: [@https://twitter.com/spiceywasabi](https://twitter.com/spiceywasabi)

### Description:

Using no existing external infrastructure we dive into the successes and failures as we crossed wires, consoled, and dial-in to real Hyosung ATMs in an effort to become a payment processor. This talk explores the approaches and techniques behind the efforts of hacking ATM systems.

## DC - Friday - 11:30-11:50 PDT

---

**Title:** Running Rootkits Like A Nation-State Hacker

**When:** Friday, Aug 12, 11:30 - 11:50 PDT

**Where:** Caesars Forum - Alliance 301-309, 321 (Track 4)

**SpeakerBio:** Omri Misgav , CTO, Security Research Group Fortinet

Omri has over a decade of experience in cyber-security. He serves as the CTO of a security research group at Fortinet focused on OS internals, malware and vulnerabilities and spearheads development of new offensive and defensive techniques. Prior to Fortinet, Omri was the security research team leader at enSilo. Before that, He led the R&D of unique network and endpoint security products for large-scale enterprise environments and was part of an incident response team, conducting investigations and hunting for nation-state threat actors.

### Description:

Code Integrity is a threat protection feature first introduced by Microsoft over 15 years ago. On x64-based versions of Windows, kernel drivers must be digitally signed and checked each time they are loaded into memory. This is also referred to as Driver Signature Enforcement (DSE).

The passing year showed high-profile APT groups kept leveraging the well-known tampering technique to disable DSE on runtime. Meanwhile, Microsoft rolled out new mitigations: driver blocklists and Kernel Data Protection (KDP), a new platform security technology for preventing data-oriented attacks.

Since using blocklist only narrows the attack vector, we focused on how KDP was applied in this case to eliminate the attack surface.

We found two novel data-based attacks to bypass KDP-protected DSE, one of which is feasible in real-world scenarios. Furthermore, they work on all Windows versions, starting with the first release of DSE. We'll present each method and run them on live machines.

We'll discuss why KDP is an ineffective mitigation. As it didn't raise the bar against DSE tampering, we looked for a different approach to mitigate it. We'll talk about how defenders can take a page out of attackers' playbook to cope with the issue until HVCI becomes prevalent and really eliminates this attack surface.

---

## LPV - Sunday - 11:00-11:45 PDT

---

**Title:** Safecracking for Everyone

**When:** Sunday, Aug 14, 11:00 - 11:45 PDT

**Where:** Caesars Forum - Summit 203-204, 235

**SpeakerBio:** Jared Dygert

No BIO available

### Description:

Safecracking is a more obscure art of locksport and this talk will cover types of safe locks, how they work, and how to defeat them.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## ASV - Friday - 10:00-16:59 PDT

---

**Title:** Satellite Eavesdropping with DDS

**When:** Friday, Aug 12, 10:00 - 16:59 PDT

**Where:** Caesars Forum - Forum 112-117

### Description:

Satellite communications are used by millions of people every day. From television broadcasts to internet services, satellites bring connectivity beyond the reach of wired infrastructure. In this lab, you'll learn about one of the most popular satellite communications protocols – DVB-S (Digital Video Broadcasting for Satellite) – and how anyone with inexpensive radio equipment and freely available software can intercept and listen to these signals.

Required gear: none!

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## ASV - Saturday - 10:00-16:59 PDT

---

**Title:** Satellite Eavesdropping with DDS

**When:** Saturday, Aug 13, 10:00 - 16:59 PDT

**Where:** Caesars Forum - Forum 112-117

### Description:

Satellite communications are used by millions of people every day. From television broadcasts to internet services, satellites bring connectivity beyond the reach of wired infrastructure. In this lab, you'll learn about one of the most popular satellite communications protocols – DVB-S (Digital Video Broadcasting for Satellite) – and how anyone with inexpensive radio equipment and freely available software can intercept and listen to these signals.

Required gear: none!

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## ASV - Sunday - 10:00-12:59 PDT

---

**Title:** Satellite Eavesdropping with DDS

**When:** Sunday, Aug 14, 10:00 - 12:59 PDT

**Where:** Caesars Forum - Forum 112-117

### Description:

Satellite communications are used by millions of people every day. From television broadcasts to internet services, satellites

bring connectivity beyond the reach of wired infrastructure. In this lab, you'll learn about one of the most popular satellite communications protocols – DVB-S (Digital Video Broadcasting for Satellite) – and how anyone with inexpensive radio equipment and freely available software can intercept and listen to these signals.

Required gear: none!

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## DC - Sunday - 11:00-11:45 PDT

---

**Title:** Save The Environment (Variable): Hijacking Legitimate Applications with a Minimal Footprint

**When:** Sunday, Aug 14, 11:00 - 11:45 PDT

**Where:** Caesars Forum - Academy 401-410, 421 (Track 3)

**SpeakerBio:** Wietze Beukema , Threat Detection & Response at CrowdStrike

Wietze has been hacking around with computers for years. Originally from the Netherlands, he currently works in Threat Detection & Response at CrowdStrike in London. As a threat hunting enthusiast and security researcher, he has presented his findings on topics including attacker emulation, command-line obfuscation and DLL Hijacking at a variety of security conferences. By sharing his research, publishing related tools and his involvement in the open source LOLBAS project, he aims to give back to the community he learnt so much from.

Twitter: [@https://twitter.com/wietze](https://twitter.com/wietze)

### Description:

DLL Hijacking, being a well-known technique for executing malicious payloads via trusted executables, has been scrutinised extensively, to the point where defensive measures are in a much better position to detect abuse. To bypass detection, stealthier and harder-to-detect alternatives need to come into play.

In this presentation, we will take a closer look at how process-level Environment Variables can be abused for taking over legitimate applications. Taking a systemic approach, we will demonstrate that over 80 Windows-native executables are vulnerable to this special type of DLL Hijacking. As this raises additional opportunities for User Account Control (UAC) bypass and Privilege Escalation, we will discuss the value and further implications of this technique and these findings.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## DC - Saturday - 10:00-10:45 PDT

---

**Title:** Scaling the Security Researcher to Eliminate OSS Vulnerabilities Once and For All

**When:** Saturday, Aug 13, 10:00 - 10:45 PDT

**Where:** Caesars Forum - Academy 401-410, 421 (Track 3)

**SpeakerBio:** Jonathan Leitschuh , OSS Security Researcher - Dan Kaminsky Fellowship @ HUMAN Security

Jonathan Leitschuh is a Software Engineer and Software Security Researcher. He is the first ever Dan Kaminsky Fellow. Jonathan is best known for his July 2019 bombshell Zoom 0-day vulnerability disclosure. He is amongst the top OSS researchers on GitHub by advisory credit. He's both a GitHub Star and a GitHub Security Ambassador. In 2019 he championed an industry-wide initiative to get all major artifact servers in the JVM ecosystem to formally decommission the support of HTTP in favor of HTTPS only. In his free time he loves rock climbing, surfing, and sailing his Hobie catamaran.

This work is sponsored by the new Dan Kaminsky Fellowship which celebrates Dan's memory and legacy by funding OSS work that makes the world a better (and more secure) place.

Twitter: [@https://twitter.com/JLLeitschuh](https://twitter.com/JLLeitschuh)

## Description:

Hundreds of thousands of human hours are invested every year in finding common security vulnerabilities with relatively simple fixes. These vulnerabilities aren't sexy, cool, or new, we've known about them for years, but they're everywhere!

The scale of GitHub & tools like CodeQL (GitHub's code query language) enable one to scan for vulnerabilities across hundreds of thousands of OSS projects, but the challenge is how to scale the triaging, reporting, and fixing. Simply automating the creation of thousands of bug reports by itself isn't useful, & would be even more of a burden on volunteer maintainers of OSS projects. Ideally the maintainers would be provided with not only information about the vulnerability, but also a fix in the form of an easily actionable pull request.

When facing a problem of this scale, what is the most efficient way to leverage researcher knowledge to fix the most vulnerabilities across OSS? This talk will cover a highly scalable solution - automated bulk pull request generation. We'll discuss the practical applications of this technique on real world OSS projects. We'll also cover technologies like CodeQL & OpenRewrite (a style-preserving refactoring tool created at Netflix & now developed by Moderne). Let's not just talk about vulnerabilities, let's actually fix them at scale.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## BHV - Saturday - 15:00-15:30 PDT

---

**Title:** Secure by Design - Facilities design cybersecurity

**When:** Saturday, Aug 13, 15:00 - 15:30 PDT

**Where:** Flamingo - Laughlin I,II,III

### SpeakerBio:

David Brearley (GICSP, PMP) is a senior professional associate and Operational Technology Cybersecurity Director at HDR. David has nearly 20 years of international experience in providing IT & OT solutions, services, and consulting covering the comprehensive control system lifecycle.

## Description:

""This presentation is on planning for cybersecurity risks that are inherent within healthcare facility control systems. Traditional standalone OT systems that operate our building (HVAC, electrical, etc) are systems are essential components to a typical healthcare facility's operation.

The evolution and market demand for smart and sustainable buildings is driving convergence of IT, IoT and OT systems. The return on investment offered by these technologies could be eliminated by a single cyber event without planning for cybersecurity and resilience, or even worse, can affect patient life safety due to interdependencies of systems.

This presentation shows how to recognize potential cybersecurity risks from integrated control system technologies and data integration, and how owners have successfully implemented secure, resilient, and maintainable solutions through application of a risk management framework within facility design."""

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

**Title:** Securing and Standardizing Data Rights Requests with a Data Rights Protocol

**When:** Friday, Aug 12, 14:00 - 14:30 PDT

**Where:** Flamingo - Vista Ballroom

**Speakers:**Ginny Fahs,Ryan Rix,Dazza Greenwood

**SpeakerBio:**Ginny Fahs

Ginny Fahs leads Product R&D at Consumer Reports Digital Lab, where she oversees a team building innovative tools and services for digital consumer protection. Her group is currently pioneering new ways for consumers to take control of their data and digital lives.

**SpeakerBio:**Ryan Rix

Ryan Rix is the Technical Lead for the Data Rights Protocol. His background is in web application development, decentralized open source software, “big tech” data rights systems, and privacy engineering.

**SpeakerBio:**Dazza Greenwood

Dazza Greenwood is the Protocol Lead for Data Rights Protocol and the founder of CIVICS.com, a boutique consultancy for legal technologies, automated transactions, data management, digital identity, and technology strategy. Dazza is also a researcher at MIT Media Lab where he is advancing the field of computational law and serves as Executive Director of the law.MIT.edu research portfolio.

**Description:**

There is no standard and secure way to exchange data rights requests under the law and it's hard and time-consuming for consumers and companies alike. We think there should be a better way to process data rights requests that's streamlined and inexpensive. A standard protocol that formalizes the components of a data rights request would allow for more consistency and efficiency for both consumers submitting requests and companies processing them. That's why Consumer Reports is incubating a Data Rights Protocol with a consortium of companies committed to strengthening consumer data rights.

Authorized agents, privacy infrastructure providers, and businesses that need to comply with CCPA will all be evaluating this protocol for its security before deciding to adopt. In this presentation our team of lawyers, technologists, and designers will enumerate security considerations for the protocol and present a draft security model that can help drive an ecosystem of products that empower consumers.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

**WS - Friday - 15:00-18:59 PDT**

---

**Title:** Securing Industrial Control Systems from the core: PLC secure coding practices

**When:** Friday, Aug 12, 15:00 - 18:59 PDT

**Where:** Harrah's - Ely

**Speakers:**Arnaud Soullie,Alexandrine Torrents

**SpeakerBio:**Arnaud Soullie , Senior Manager

Arnaud Soullié (@arnaudsoullie) is a Senior Manager at Wavestone, a global consulting company. For 12 years, he has been performing security assessments and pentests on all types of targets. He started specializing in ICS cybersecurity 10 years ago. He spoke and taught workshops at numerous security conferences on ICS topics : BlackHat Europe, BruCon, CS3STHLM, BSides Las Vegas, DEFCON... He is also the creator of the DYODE project, an open-source data diode aimed at ICS. He has been teaching ICS cybersecurity training since 2015.

Twitter: [@https://twitter.com/arnaudsoullie](https://twitter.com/arnaudsoullie)

## **SpeakerBio:**Alexandrine Torrents , Security Consultant

Alexandrine Torrents is a cybersecurity consultant at Wavestone, a French consulting company. She started as a penetration tester, and performed several cybersecurity assessments on ICS. She worked on a few ICS models to demonstrate attacks on PLCs and developed a particular tool to request Siemens PLCs. Then, she started working at securing ICS, especially in the scope of the French military law, helping companies offering a vital service to the nation to comply with security rules. Now, Alexandrine works with different industrial CISOs on their cybersecurity projects: defining secure architectures, hardening systems, implementing detection mechanisms. She is also IEC 62443 certified and still performs assessments on multiple environments.

## **Description:**

Securing Industrial Control Systems from cyberattacks often starts by properly segmenting the network, securing remote accesses and overall focusing on traditional “IT” cybersecurity measures. However, we can also leverage existing technology to detect and protect from cyberattacks. The Top 20 Secure PLC Coding Practices ([www.plc-security.com](http://www.plc-security.com)) is a community-led effort to identify best practices in Programmable Logic Controllers (PLC) code development that improve cybersecurity. In this workshop, you will learn how to program a PLC and connect it to a SCADA system. You will then perform attacks on this system and finally implement a sample of the TOP20 coding practices to block or detect such attacks. You will be provided with access to cloud VMs preconfigured with a SCADA software as well as a PLC simulator. Some demonstrations will also be performed on-site on real hardware PLCs.

The workshop is accessible to anyone, even with no prior ICS experience.

### Materials

Just a laptop with a modern web browser. Students will be provided with cloud VMs to perform the exercises

### Prereq

None

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## **WS - Friday - 15:00-18:59 PDT**

---

**Title:** Securing Smart Contracts

**When:** Friday, Aug 12, 15:00 - 18:59 PDT

**Where:** Harrah's - Reno

**Speakers:**Irvin Lemus,Kaitlyn Handelman,Elizabeth Biddlecome,Sam Bowne

### **SpeakerBio:**Irvin Lemus , Instructor

Irvin Lemus has been in the industry for 10+ years as an MSP technician, consultant, instructor and coordinator. He is currently the cybersecurity professor at Cabrillo College in Santa Cruz, CA. He also is the Bay Area Cyber Competitions Regional Coordinator as well as the contest creator for SkillsUSA CA and FL. Irvin has spoken at various cybersecurity and educational conferences. Irvin holds a CISSP and a Bachelor's Degree in Information Security.

### **SpeakerBio:**Kaitlyn Handelman , Security Engineer

Kaitlyn Handelman is a security engineer and consultant, defending high-value networks professionally. She has extensive experience in aerospace, radio, and hardware hacking.

Industry credentials: OSCP, OSED

### **SpeakerBio:**Elizabeth Biddlecome , Consultant and Instructor

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 scripting languages in cybersecurity competitions, hackathons, and CTFs.

### **SpeakerBio:**Sam Bowne , Instructor

Sam Bowne has been teaching computer networking and security classes at City College San Francisco since 2000, and is the founder of Infosec Decoded, Inc. He has given talks and hands-on trainings at Black Hat USA, RSA, DEF CON, DEF CON China, HOPE, and many other conferences.

Credentials: PhD, CISSP, DEF CON Black Badge Co-Winner

### **Description:**

Learn how blockchains, cryptocurrency, NFTs, and smart contracts work, and their most important security flaws. We will also cover the underlying cryptography: hashes, symmetric encryption, and asymmetric encryption. We will configure wallets, servers, and vulnerable smart contracts, and exploit them.

We will configure systems using Bitcoin, Ethereum, Hyperledger, Multichain, Stellar, and more. We will perform exploits including double-spend, reentrancy, integer underflow, and logic flaws.

No previous experience with coding or blockchains is required.

This workshop is structured as a CTF competition, to make it useful to students at all levels. We will demonstrate the easier challenges from each topic, and detailed step-by-step instructions are available. We will have several instructors available to answer questions and help participants individually. Every participant should learn new, useful techniques.

#### Materials

Any computer with a Web browser. The capacity to run a local virtual machine is helpful but not required.

#### Prereq

Beginners are welcome. Familiarity with cryptocurrency and smart contracts is helpful but not necessary.

---

[Return to Index](#) - Add to



- ics [Calendar](#) file

---

## **ASV - Friday - 13:30-13:55 PDT**

---

**Title:** Securing the Future of Aviation CyberSecurity

**When:** Friday, Aug 12, 13:30 - 13:55 PDT

**Where:** Caesars Forum - Forum 112-117

### **SpeakerBio:**Timothy Weston , Deputy Executive Director (acting), Cybersecurity Policy Coordinator, Transportation Security Administration

Tim Weston is the Director for Strategy & Performance in TSA's office of Strategy, Policy Coordination and Innovation. Mr. Weston also serves as the TSA Cybersecurity Policy Coordinator. Previously, he worked in the TSA Office of Chief Counsel, as Senior Counsel in the Security Threat Assessment Division.

### **Description:**

Presentation will cover the future of aviation cybersecurity, including the security of Advanced Air Mobility/Urban Air Mobility, Space Port Security, Space Tourism Security, and the transformation of the TSA workforce. I will cover in depth the legal and regulatory framework that provides for securing IT and OT networks, as well as the airframes, for the next generation of air travel. I will close with an update and call for action to modernization of the aviation workforce.

## WS - Saturday - 15:00-18:59 PDT

---

**Title:** Securing Web Apps

**When:** Saturday, Aug 13, 15:00 - 18:59 PDT

**Where:** Harrah's - Reno

**Speakers:**Elizabeth Biddlecome,Kaitlyn Handelman,Irvin Lemus,Sam Bowne

**SpeakerBio:**Elizabeth Biddlecome , Consultant and Instructor

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 scripting languages in cybersecurity competitions, hackathons, and CTFs.

**SpeakerBio:**Kaitlyn Handelman , Security Engineer

Kaitlyn Handelman is a security engineer and consultant, defending high-value networks professionally. She has extensive experience in aerospace, radio, and hardware hacking.

Industry credentials: OSCP, OSED

**SpeakerBio:**Irvin Lemus , Instructor

Irvin Lemus has been in the industry for 10+ years as an MSP technician, consultant, instructor and coordinator. He is currently the cybersecurity professor at Cabrillo College in Santa Cruz, CA. He also is the Bay Area Cyber Competitions Regional Coordinator as well as the contest creator for SkillsUSA CA and FL. Irvin has spoken at various cybersecurity and educational conferences. Irvin holds a CISSP and a Bachelor's Degree in Information Security.

**SpeakerBio:**Sam Bowne , Instructor

Sam Bowne has been teaching computer networking and security classes at City College San Francisco since 2000, and is the founder of Infosec Decoded, Inc. He has given talks and hands-on trainings at Black Hat USA, RSA, DEF CON, DEF CON China, HOPE, and many other conferences.

Credentials: PhD, CISSP, DEF CON Black Badge Co-Winner

### Description:

Attack Web applications with: command injection, SQL injection, Cross-Site Request Forgery, Cross-Site Scripting, cookie manipulation, Server-Side Template Injection, and more. We will also exploit Drupal and SAML. We will then implement network defenses and monitoring agents. We will use Burp, Splunk, and Suricata. We will also perform attacks on a vulnerable API. This workshop is structured as a CTF competition, to make it useful to students at all levels. We will demonstrate the easier challenges from each topic, and detailed step-by-step instructions are available. We will have several instructors available to answer questions and help participants individually. Every participant should learn new, useful techniques.

### Materials

Any computer with a Web browser.

### Prereq

Beginners are welcome. Familiarity with web technologies is helpful but not necessary.

## CLV - Friday - 13:10-13:40 PDT

**Title:** Security at Every Step: The TL;DR on Securing Your AWS Code Pipeline

**When:** Friday, Aug 12, 13:10 - 13:40 PDT

**Where:** Flamingo - Scenic Ballroom

**SpeakerBio:**Cassandra Young (muteki)

Cassandra (aka muteki) works full time in information security consulting, specializing in Cloud Security Architecture and Engineering. She holds a master's degree in Computer Science, focusing on cloud-based app development and academic research on serverless security and privacy/anonymity technology. Additionally, as one of the directors of Blue Team Village, Cassandra works to bring free Blue Team talks, workshops and more to the broader security community.

Twitter: [@https://twitter.com/muteki\\_rtw](https://twitter.com/muteki_rtw)

**Description:**

Securing application or infrastructure code in the Cloud is more than just scoping permissions in IAM and scanning ECS, EKS and EC2 instances. Attackers can use poisoned container instances, malicious code and dependencies, and vulnerable CI/CD pipelines to break into your environment, requiring you to consider the entire development lifecycle, from who's writing the code, to how it's deployed. This short talk will introduce you to basic but powerful practices you can put in place now, such as signed Git commits, securing repo access, code analysis, CI/CD permissions, and resource scanning and hardening.

## CLV - Saturday - 12:30-13:10 PDT

**Title:** Security Misconfigurations in the Cloud - "Oh Look, something fluffy, poke, poke, poke"

**When:** Saturday, Aug 13, 12:30 - 13:10 PDT

**Where:** Flamingo - Scenic Ballroom

**SpeakerBio:**Kat Fitzgerald

Based in Seattle and a natural creature of winter, you can typically find me sipping Grand Mayan Extra Anejo whilst simultaneously defending my systems using OSS, magic spells and Dancing Flamingos. HoneyPots & Refrigerators are a few of my favorite things! Fun Fact: I rescue Feral Pop Tarts and have the only Pop Tart Sanctuary in the Seattle area.

Twitter: [@https://twitter.com/rnbwkat](https://twitter.com/rnbwkat)

**Description:**

Intro time (5 mins) Well, I have to say who I am and why I'm here and my qualifications, otherwise people leave. Ok, maybe they don't leave, but I want to explain how/why I do this and how I'm going to make it a fun project for everyone after the talk! Baking something fluffy (10 mins) Now I take a few minutes to explain the common concepts of cloud configurations such as IAM/ORG policies and how they compare to redteaming 'on-prem'. It's all about understanding the magic that is the cloud in clear terms that everyone can follow along with - and yes, there are funny jokes and memes throughout. A happy crowd is an engaged crowd! Seriously, in a quick 10 minutes, 'Pizza as a Service' is used to explain the concepts of the cloud, the attack vectors presented and how pentesters and bad actors use these attack points to their advantage. It's clobberin time (10 mins) Let's get to it with lots of example of misconfigurations and the attack vectors they pose. This is both live (with recorded backup) demo time and OSS tool demonstrations to help find misconfigured cloud services. Not much else to say about this part. It is interactive, fun and really shows off how simple mistakes can lead to serious incidents like exposing

millions of records to the public 'accidentally' or how a public github repo was used to launch over 300 VMs for crypto mining and no one knew until a month later. Oh yeah, and a brief description of how cryptomining is a fun diversion to take your attention away from what the attacker was really doing will be discussed. Peace offerings to the demo gods will be made prior to the live portion of course. Great, now how do we fix it? (10 mins) Well, attendees have to come away with some clear AIs to be able to apply to their cloud configurations and some suggestions on how to avoid misconfigurations in the first place. Auditing tools are discussed and shown (not in demo, but output from audits are shared and discussed) Tools discussed are all OSS and nothing, (and I mean nothing!) is commercial! Before and afters of misconfigured cloud projects will be shown with some general automation suggestions to help remove the 'human threat' factor from the process. Key Takeaways (5 mins) Let's bring it all to a neat and tidy conclusion with specific takeaways so attendees feel like they got something out of this. What good is any talk without identified specifics of what we learned and how to apply them, am I right? And there you have it, tied up neatly with a lovely bow and ready to take home! Q/A (5 mins)

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## ASV - Sunday - 10:00-10:25 PDT

---

**Title:** Self No-Fly Area Designing for UAV

**When:** Sunday, Aug 14, 10:00 - 10:25 PDT

**Where:** Caesars Forum - Forum 112-117

**SpeakerBio:**Utku Yildirim , Red Teamer / Penetration Tester

Utku Yildirim is Red Teamer / Penetration Tester at Hoffmann Cybersecurity Netherlands. He is a computer engineer and MSc student in Cyber Security. He has multiple red team certificates such as OSCE, OSCP, OSWP and LPT. Utku has spoken at international congresses before DEF CON 30.

### Description:

His method is able to create a no-fly area by spreading signals that can display the coordinates of any selected area as airport GPS coordinates with multiple HackRF. With this method, you can ensure security and privacy by closing the desired areas from public areas such as homes, workplaces etc.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## DL - Saturday - 12:00-13:55 PDT

---

**Title:** SharpSCCM

**When:** Saturday, Aug 13, 12:00 - 13:55 PDT

**Where:** Caesars Forum - Society Boardroom

**Speakers:**Chris Thompson,Duane Michael

**SpeakerBio:**Chris Thompson

Chris is a senior consultant on SpecterOps's adversary simulation team and has over ten years of experience in information security, serving numerous Fortune 500 clients in the retail, consumer products, financial, and telecom industries. He has extensive experience leading network, web application, and wireless penetration tests, social engineering engagements, and technical security assessments to provide actionable recommendations that align with each organization's security strategy and risk tolerance. Chris enjoys researching and applying new tradecraft to overcome technical challenges and writing tools that automate tasks and improve efficiency.

**SpeakerBio:**Duane Michael

Duane is a senior consultant on SpecterOps's adversary simulation team, where he conducts advanced red team exercises and instructs courses on red team operations and vulnerability research. He has over ten years of experience in information security, with a deep curiosity for researching Windows, its internals, and related technologies. Duane strives to demystify tradecraft for clients through both an offensive and defensive lens, an activity he has performed for numerous Fortune 100 clients.

## Description:

SharpSCCM is a post-exploitation tool designed to leverage Microsoft Endpoint Configuration Manager (a.k.a. ConfigMgr, formerly SCCM) for lateral movement from a C2 agent without requiring access to the SCCM administration console. SharpSCCM supports lateral movement functions ported from PowerSCCM and contains additional functionality to abuse newly discovered attack primitives for coercing NTLM authentication from local administrator and SCCM site server machine accounts in environments where automatic client push installation is enabled. SharpSCCM can also dump information about the SCCM environment from a client, including domain credentials for Network Access Accounts. Further, with access to an SCCM administrator account, operators of SharpSCCM can execute code as SYSTEM or coerce NTLM authentication from the currently logged-in user or the machine account on any SCCM client.

Audience: Offense, Defense, System Administrators

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## CLV - Friday - 14:20-14:50 PDT

---

**Title:** Shopping for Vulnerabilities - How Cloud Service Provider Marketplaces can Help White and Black Hat Vulnerability Research

**When:** Friday, Aug 12, 14:20 - 14:50 PDT

**Where:** Flamingo - Scenic Ballroom

### SpeakerBio: Alexandre Sieira

Alexandre (or Alex) Sieira is a successful information security entrepreneur in the information security field with a global footprint since 2003. He began his security career as a Co-Founder and CTO of CIPHER, an international security consulting and MSSP headquartered in Brazil which was later acquired by Prosegur. In 2015, he became Co-Founder and CTO of Niddel, a bootstrapped security analytics SaaS startup running entirely on the cloud, which was awarded a Gartner Cool Vendor award in 2016. After the acquisition of Niddel by Verizon in January 2018, he became the Senior manager and global leader of the Managed Security Services - analytics products under the Detect & Respond portfolio tower at Verizon. Currently is the CEO and Co-Founder of Tenchi Security, a company focused on cloud security.

Alex is also an experienced speaker having presented at Black Hat, BSides SF, FIRST Conference, DEF CON Cloud Village and local events in Brazil several times over his career.

Twitter: [@https://twitter.com/AlexandreSieira](https://twitter.com/AlexandreSieira)

## Description:

Recently the Conti ransomware group internal chat leaks was fascinating reading. Among other things, it reminded us that both well-intentioned and malicious actors are constantly trying to find ways to find vulnerabilities and develop exploits to widely used IT products. This is particularly true those that are externally exposed firewalls, VPNs and load balancers, or security products that might thwart their techniques and tools. The timeline from the chats seems to show a gap of several months between Conti members trying to procure either appliances or commercial software that they were trying to get for these purposes. This got us thinking about how the major cloud service providers these days have marketplaces where you can easily buy virtual appliances or SaaS licenses for lots of widely used IT and security products with little more than a valid credit card, in minutes. And we decided to check how feasible it is to use this to conduct vulnerability research. In this presentation we will show what kind of access one can get to the internals of IT and security products using these

marketplaces, particularly in the case of products only typically offered in hardware appliances. Which cloud providers try to prevent this sort of activity, how they do it, which ones simply don't care, and what techniques we were able to use to access these appliance's internals. The objective here is threefold: 1) help well intentioned vulnerability researchers find an easier avenue to do their work; 2) allow cloud providers to get a better understanding of how their marketplaces can be abused and which controls they could implement to mitigate that risk, and 3) let IT and security vendors realize the added exposure of publishing their products on these marketplaces.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## CLV - Sunday - 12:30-12:50 PDT

---

**Title:** Sign of the Times: Exploiting Poor Validation of AWS SNS SigningCertUrl

**When:** Sunday, Aug 14, 12:30 - 12:50 PDT

**Where:** Flamingo - Scenic Ballroom

**SpeakerBio:** Eugene Lim , Cybersecurity Specialist, Government Technology Agency of Singapore

Eugene (spaceraccoon) hacks for good! At GovTech Singapore, he protects citizen data and government systems through security research. He also develops SecOps integrations to secure code at scale. He recently reported remote code execution vulnerabilities in Microsoft Office and Apache OpenOffice and discussed defensive coding techniques he observed from hacking Synology Network Attached Storage devices at ShmooCon.

As a bug hunter, he helps secure products globally, from Amazon to Zendesk. In 2021, he was selected from a pool of 1 million registered hackers for HackerOne's H1-Elite Hall of Fame. Besides bug hunting, he builds security tools, including a malicious npm package scanner and a social engineering honeypot that were presented at Black Hat Arsenal. He writes about his research on <https://spaceraccoon.dev>.

He enjoys tinkering with new technologies. He presented "Hacking Humans with AI as a Service" at DEF CON 29 and attended IBM's Qiskit Global Quantum Machine Learning Summer School.

Twitter: [@https://twitter.com/spaceraccoonsec](https://twitter.com/spaceraccoonsec)

### Description:

Countless projects rely on Amazon Web Services' Simple Notification Service for application-to-application communication such as webhooks and callbacks. To verify the authenticity of these messages, these projects use certificate-based signature validation based on the SigningCertURL value. Unfortunately, developers are tasked with verifying the authenticity of the certificate URL themselves, creating a vulnerable-by-default 'configuration over convention' situation that spawns numerous vulnerabilities. This is an official design pattern recommended by AWS itself (<https://docs.aws.amazon.com/sns/latest/dg/sns-verify-signature-of-message.html>). I will demonstrate how various custom checks and regexes in real projects can be bypassed to forge SNS messages by leveraging a namespace clash with Amazon S3. Attackers can generate and host their own public keys on S3 buckets that pass custom verification checks, allowing them to trigger sensitive webhook functionality. In addition, I will go further to discuss a key loophole (pending disclosure) in official AWS SDKs like sns-validator that affects all downstream dependents, from Firefox Monitor to the 70 million download/week Definitely Typed package. I will dive into possible short-, medium-, and long-term fixes pending AWS' own patch. As a result, attendees will walk away with a better understanding of the difficulties in securing trusted application-to-application cloud messaging tools. I will discuss how to code defensively by going for convention over configuration in cloud architecture. I will also provide pointers on discovering vulnerable SNS webhook implementations through code review.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

**Title:** SimPPL: Simulating Social Networks and Disinformation

**When:** Friday, Aug 12, 11:30 - 13:30 PDT

**Where:** Caesars Forum - Summit 221->236

**SpeakerBio:** Swapneel Mehta

Swapneel Mehta is a Ph.D. student at NYU Data Science working with the Center for Social Media and Politics (<https://csmapnyu.org/>) and collaborating with researchers at Oxford University. His research deals with controlling misinformation on social networks using tools from simulation-based inference and causality, using probabilistic programs to simulate user behavior and information propagation on social networks. He is also a co-founder of SimPPL, a non-profit venture to support independent local journalists and local news understand and cater to their digital audiences, the founder and leader at Unicode Research (<https://unicode-research.netlify.app/people>), and recently taught a Google-backed independent ML Summer Course (<https://djunicode.github.io/umlsc-2021/>).

**Description:** No Description available

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## PWV - Saturday - 11:00-10:59 PDT

---

**Title:** So long, PBKDF2! The end of password-based key derivation

**When:** Saturday, Aug 13, 11:00 - 10:59 PDT

**Where:** Caesars Forum - Summit 218-219

**SpeakerBio:** Vivek Nair

Vivek Nair is an EECS Ph.D. student at UC Berkeley and a researcher at Cornell's IC3. As a recipient of the NSF, NPSC, and Hertz fellowships, Vivek has worked with the US Department of Defense to build resilient cyber systems. He began researching cybersecurity in 2015, when he founded Multifactor.com, and has gone on to author 12+ patents for cybersecurity technologies. He was the youngest-ever recipient of Bachelor's and Master's degrees in Computer Science at the University of Illinois at the ages of 18 and 19 respectively. Outside of cybersecurity, Vivek is a competitive VR eSports player and the captain of UC Berkeley's Beat Saber team, which he led to a US collegiate championship victory in 2021.

**Description:**

"From Apple iOS to LastPass to WPA/WPA2, decades-old password-based key derivation functions like PBKDF2 remain in widespread use across major enterprise systems today. Yet the advent of fast SHA-1 and SHA-256 ASICs and the increasing prevalence of credential stuffing and password spraying attacks have made password-based key derivation all but obsolete. Moreover, current key recovery standards (like NIST SP 800-57) suggest using a master key to recover lost passwords, creating a central point of failure and thus entirely defeating the purpose of user-derived keys. While multi-factor authentication is a great defense against credential stuffing, password-derived keys remain only as strong as the passwords they're based on. This talk will demonstrate how credential stuffing attacks can target data encrypted with password-derived keys and will propose a new KDF construction, ""multi-factor key derivation,"" that leverages novel cryptography to take advantage of all of a user's authentication factors in the key derivation process."

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## DC - Sunday - 14:00-14:45 PDT

---

**Title:** Solana JIT: Lessons from fuzzing a smart-contract compiler

**When:** Sunday, Aug 14, 14:00 - 14:45 PDT

**Where:** Caesars Forum - Alliance 301-309, 321 (Track 4)

### **SpeakerBio:** Thomas Roth

Thomas Roth is a security researcher from Germany. In the past he has published research on topics like TrustZone, fault injection, payment terminals, cryptocurrency-wallets and embedded security.

### **Description:**

Solana is a blockchain with a \$37 billion dollar market cap with the security of that chain relying on the security of the smart contracts on the chain - and we found very little research on the actual execution environment of those contracts. In contrast to Ethereum, where contracts are mostly written in Solidity and then compiled to the Ethereum Virtual Machine, Solana uses a different approach: Solana contracts can be written in C, Rust, and C++, and are compiled to eBPF. Underneath the hood, Solana uses rBPF: A Rust BPF implementation with a just-in-time compiler. Given the security history of eBPF in the Linux kernel, and the lack of previous public, low-level Solana research, we decided to dig deeper: We built Solana reverse-engineering tooling and fuzzing harnesses as we slowly dug our way into the JIT - eventually discovering multiple out-of-bounds vulnerabilities.

---

[Return to Index](#) - Add to



- ics [Calendar](#) file

---

## DC - Friday - 14:00-14:45 PDT

---

**Title:** Space Jam: Exploring Radio Frequency Attacks in Outer Space

**When:** Friday, Aug 12, 14:00 - 14:45 PDT

**Where:** Caesars Forum - Forum 104-105, 135-136 (Track 1)

### **SpeakerBio:** James Pavur , Digital Service Expert, Defense Digital Service

Dr. James Pavur is a Digital Service Expert at the DoD Directorate of Digital Services where he advises and assists the US Department of Defense in implementing modern digital solutions to urgent and novel challenges. Prior to joining DDS, James received his PhD. from Oxford University's Department of Computer Science as a Rhodes Scholar. His thesis "Securing New Space: On Satellite Cybersecurity" focused on the security of modern space platforms - with a particular interest in vulnerability identification and remediation. His previous research on satellite security has been published at top academic venues, such as IEEE S&P and NDSS, presented at major cybersecurity conferences, including Black Hat USA and DEFCON, and covered in the popular press. Outside of tech, James enjoys flying kites and collecting rare and interesting teas.

Twitter: [@https://twitter.com/jamespavur](https://twitter.com/jamespavur)

### **Description:**

Satellite designs are myriad as stars in the sky, but one common denominator across all modern missions is their dependency on long-distance radio links. In this briefing, we will turn a hacker's eye towards the signals that are the lifeblood of space missions. We'll learn how both state and non-state actors can, and have, executed physical-layer attacks on satellite communications systems and what their motivations have been for causing such disruption.

Building on this foundation, we'll present modern evolutions of these attack strategies which can threaten next-generation space missions. From jamming, to spoofing, to signal hijacking, we'll see how radio links represent a key attack surface for space platforms and how technological developments make these attacks ever more accessible and affordable. We'll simulate strategies attackers may use to cause disruption in key space communications links and even model attacks which may undermine critical safety controls involved in rocket launches.

The presentation will conclude with a discussion of strategies which can defend against many of these attacks.

While this talk includes technical components, it is intended to be accessible to all audiences and does not assume any prior background in radio communications, astrodynamics, or aerospace engineering. The hope is to provide a launchpad for researchers across the security community to contribute to protecting critical infrastructure in space and beyond.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## ASV - Saturday - 16:00-16:50 PDT

---

**Title:** Space ISAC: Protecting Our Space Assets

**When:** Saturday, Aug 13, 16:00 - 16:50 PDT

**Where:** Caesars Forum - Forum 112-117

### Description:

Erin Miller, the Executive Director of Space ISAC, will lead a panel discussing the trends, data, intelligence, and threats that are affecting space systems and the satellite community.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## CLV - Saturday - 12:00-12:30 PDT

---

**Title:** SquarePhish - Phishing Office 365 using QR Codes and OAuth 2.0 Device Code Flow

**When:** Saturday, Aug 13, 12:00 - 12:30 PDT

**Where:** Flamingo - Scenic Ballroom

**Speakers:**Kamron Talebzadeh,Nevada Romsdahl

### SpeakerBio:

Kamron Talebzadeh

Kam Talebzadeh is a penetration tester and security researcher. He has developed and published several open-source offensive toolkits including o365spray, BridgeKeeper, and redirect.rules. Currently, he works as a Security Researcher for Secureworks. He holds the Offensive Security WebExpert (OSWE) certification.

### SpeakerBio:

Nevada Romsdahl

Nevada Romsdahl is currently a senior security researcher for Secureworks. In his 15 year information security career, Nevada has held the roles of security analyst, security architect, penetration tester and security researcher. He holds many offensive security certifications including OSCP, OSWP, OSWE, OSCE, and OSEE.

Twitter: [@https://twitter.com/nevadaromsdahl](https://twitter.com/nevadaromsdahl)

### Description:

SquarePhish is a phishing tool that combines QR Codes and OAuth 2.0 Device Code Flow for Advanced Phishing Attacks against Office 365.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## BICV - Saturday - 13:00-13:59 PDT

---

**Title:** State of the Model

**When:** Saturday, Aug 13, 13:00 - 13:59 PDT

**Where:** Virtual - BIC Village

**Speakers:**Jovonni Pharr,GACWR Team

**SpeakerBio:**Jovonni Pharr

No BIO available

**SpeakerBio:**GACWR Team

No BIO available

**Description:**No Description available

---

[Return to Index](#) - Add to



- ics [Calendar](#) file

---

## DC - Sunday - 11:00-11:45 PDT

---

**Title:** STrace - A DTrace on windows reimplementation.

**When:** Sunday, Aug 14, 11:00 - 11:45 PDT

**Where:** Caesars Forum - Alliance 301-309, 321 (Track 4)

**SpeakerBio:**Stephen Eckels

Stephen Eckels, is a reverse engineer that explores blue team tooling and regularly sees front line malware. Stephen has published past tools such as GoReSym - a golang symbol recovery tool, and written extensively about many forms of hooking including hooking the wow64 layer. Stephen maintains the open source hooking library PolyHook, some of his other work is public on the Mandiant blog!

Twitter: [@https://twitter.com/stevemk14ebr](https://twitter.com/stevemk14ebr)

**Description:**

I'll document the kernel tracing APIs in modern versions of windows, implemented to support Microsofts' port of the 'DTrace' system to windows. This system provides an officially supported mechanism to perform system call interception that is patchguard compatible, but not secure boot compatible. Alongside the history and details of DTrace this talk will also cover a C++ and Rust based reimplementation of the system that I call STrace. This reimplementation allows users to write custom plugin dlls which are manually mapped to the kernel address space. These plugins can then log all system calls, or perform any side effects before and after system call execution by invoking the typical kernel driver APIs – if desired.

---

[Return to Index](#) - Add to



- ics [Calendar](#) file

---

## CPV - Sunday - 12:00-12:30 PDT

---

**Title:** Surviving and Designing for Survivors

**When:** Sunday, Aug 14, 12:00 - 12:30 PDT

**Where:** Flamingo - Vista Ballroom

## **SpeakerBio:**Avi Zajac

Avi (@\_llzes, Avi/they/he) is a privacy-focused hacker. They love rabbits, cheesecake, and cute things like privacy and security, locksport, cryptography. They builds mission-driven products; help individuals and organisations protect their privacy and safety; and enjoy making and breaking things for a more equitable world.

## **Description:**

The privacy and security communities spin out new technologies, platforms, policies, regulations, and other novel research rapidly in the pursuit of creating a positive impact in the world at a dizzying pace. Unfortunately, systems often behave or are used in ways that we did not intend them to. Perhaps we could have caught the potential harms associated with systems intended to protect vulnerable people had we taken a systematic approach in evaluating them. In this talk, we build up the building blocks with examples and case studies to understand the challenges many survivors face systemically and in their day-to-day lives, with resources for survivors and takeaways for practitioners.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## **DL - Saturday - 10:00-11:55 PDT**

---

**Title:** svachal + machinescli

**When:** Saturday, Aug 13, 10:00 - 11:55 PDT

**Where:** Caesars Forum - Committee Boardroom

## **SpeakerBio:**Ankur Tyagi

Ankur is working with Qualys Inc. as a Principal Engineer. On the Internet, he goes by the handle 7h3rAm and usually blogs here: <http://7h3ram.github.io/>.

## **Description:**

Writeups for CTF challenges and machines are a critical learning resource for our community. For the author, it presents an opportunity to document their methodology, tips/tricks and progress. For the audience, it serves as reference material.

Oftentimes, authors switch roles and become the audience to learn from their own work. This demo aims to showcase tools, svachal and machinescli, developed with these insights. These work in conjunction to help users curate their learning in .yml structured files, find insights and query this knowledge base as and when needed.

Audience: Offense/Defense

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## **BTV - Friday - 16:00-16:59 PDT**

---

**Title:** Take Your Security Skills From Good to Better to Best!

**When:** Friday, Aug 12, 16:00 - 16:59 PDT

**Where:** Flamingo - Savoy Ballroom - BTV Main Stage

**Speakers:**Ricky Banda,Neumann Lim (scsideath),Tracy Z. Maleeff,Kimberly Mentzell,Tanisha O'Donoghue

## **SpeakerBio:**Ricky Banda

Ricky Banda is a 28 year old SOC Incident Response Manager for ARM Semiconductors Ltd. He began his career at 16 as an intern with the United States Air Force working in the 33d Network Warfare Squadron at Lackland Airforce Base. He has worked in security operations for 12 years. In education, he is a SANS Graduate student and has 18 certifications, as well as a

bachelor's in cybersecurity. His primary focus in SecOps is to reduce SOC burnout and support security operations workers. When not working, he supports metal musicians and is an avid horror fan.

### **SpeakerBio:**Neumann Lim (scsdeath)

Neumann Lim is a manager at Deloitte where he leads the cyber detection and incident response teams. Prior to this role, Neumann spent years working with large enterprises and governments specializing in incident response.

With 15 years of infosec experience, he enjoys analyzing malware, reverse-engineering and vulnerability research. Neumann has been invited to share his thought leadership at conferences such as Grayhat Conf, Toronto CISO Summit and CCTX.

In his off time, Neumann participates in CTFs and mentors new students interested in infosec while maintaining active membership of various security organizations such as DefCon, HTCIA, ISC2 and EC-Council.

### **SpeakerBio:**Tracy Z. Maleeff

Tracy Z. Maleeff, aka InfoSecSherpa, is a Security Researcher with the Krebs Stamos Group. She previously held roles of Information Security Analyst at The New York Times Company and Cyber Analyst for GlaxoSmithKline. Prior to joining the Information Security field, Tracy worked as a librarian in academic, corporate, and law firm libraries. She holds a Master of Library & Information Science degree from the University of Pittsburgh in addition to undergraduate degrees from both Temple University (magna cum laude) and the Pennsylvania State University. Tracy publishes a daily InfoSec newsletter and OSINT blog at [infosecsherpa.medium.com](https://infosecsherpa.medium.com). Representin' the Philly jawn.

### **SpeakerBio:**Kimberly Mentzell

No BIO available

### **SpeakerBio:**Tanisha O'Donoghue

Over the last 6 years, Tanisha O'Donoghue has been on an upward climb in the Cyber Security Space. The Guyanese native resides in the Washington, DC area and works on the Information Security Compliance team at Tyler Technologies, assisting with policy management, audits, and risk management. Tanisha's career experience has included incident response/recovery, vulnerability management, risk management, and compliance. She is the Director of Policy and Procedures at BlackGirlsHack, a nonprofit organization that provides resources, training, mentoring, and opportunities to black women to increase representation and diversity in the cyber security field.

### **Description:**

Why dwell in the lobby of the Security field when you could be enjoying the view from the penthouse? Get insight from our esteemed panel on how to stay up to date on hacker news, increase your technical skills, and be aware of opportunities for professional development. Our panel will also discuss the importance of sending that elevator back down to help others so that our entire industry can grow and thrive, just like you will. Open up your ears and your mind and enjoy the gems that will be dropped.

Why dwell in the lobby of the Security field when you could be enjoying the view from the penthouse? Get insight from our esteemed panel on how to stay up to date on hacker news, increase your technical skills, and be aware of opportunities for professional development. Our panel will also discuss the importance of sending that elevator back down to help others so that our entire industry can grow and thrive, just like you will. Open up your ears and your mind and enjoy the gems that will be dropped.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

**DC - Sunday - 12:00-12:45 PDT**

---

**Title:** Taking a Dump In The Cloud

**When:** Sunday, Aug 14, 12:00 - 12:45 PDT

**Where:** Caesars Forum - Forum 106-110, 138-139 (Track 2)

**Speakers:** Flangvik, Melvin Langvik

**SpeakerBio:** Flangvik

No BIO available

**SpeakerBio:** Melvin Langvik , Security Consultant, TrustedSec Targeted Operations

Melvin started as a C Azure developer and integrations consultant after finishing his bachelor's degree in computer engineering. During his time as a developer, he got hands-on experience with rapidly creating and deploying critical backend infrastructure for an international client base. It was during this period Melvin started to pursue his goal of transitioning into offensive security. Melvin broke into the HackTheBox cybersecurity platform "Hall Of Fame" and subsequently successfully landed as a security consultant. While working as a penetration tester, Melvin has contributed to the infosec community by releasing open-source and offensively targeted C based tools and techniques, such as BetterSafetyKatz, SharpProxyLogon, AzureC2Relay, and CobaltBus. Melvin is also the creator and maintainer of the SharpCollection project, a project which utilizes Azure DevOps PipeLines to automatically release pre-compiled binaries of the most common offensive C# projects, triggered by updates from their respective main branch

Twitter: [@https://twitter.com/Flangvik](https://twitter.com/Flangvik)

### Description:

Taking a Dump In The Cloud is a tale of countless sleepless nights spent reversing and understanding the integration between Microsoft Office resources and how desktop applications implement them. The release of the TeamFiltration toolkit, connecting all the data points to more effectively launch attacks against Microsoft Azure Tenants. Understanding the lack of conditional access for non-interactive logins and how one can abuse the magic of Microsofts OAuth implementation with Single-Sign-On to exfiltrate all the loot. Streamlining the process of account enumeration and validation. Thoughts on working effectively against Azure Smart Lockout. Exploring options of vertical movement given common cloud configurations, and more!

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## SKY - Friday - 12:45-13:35 PDT

---

**Title:** Taking Down the Grid

**When:** Friday, Aug 12, 12:45 - 13:35 PDT

**Where:** LINQ - BLOQ

**SpeakerBio:** Joe Slowik

Joe Slowik has over a decade of experience across multiple facets of information security and offensive computer network operations. Currently leading threat intelligence and detection engineering work at Gigamon, Joe has previously performed cyber threat intelligence research at DomainTools and Dragos, and spent several years in both the US Department of Energy and as an Officer in the US Navy.

Twitter: [@https://twitter.com/jfslowik](https://twitter.com/jfslowik)

### Description:

Media hype concerning ""attacks"" on the electric grid is common through multiple sources, but ignores actual vectors of concern for impacting electric services to populations. This talk will examine how cyber effects can effectively impair electric services, focusing on how cyber can leverage underlying system dependencies and opportunities to achieve outsized impacts. In addition to reviewing the most studied disruptive cyber events on electric systems (2015 and 2016 Ukraine), this talk will also explore ""near miss"" events (such as the Berserk Bear campaigns from 2017 through at least 2020) as well as recent

events in Ukraine. Furthermore, we will also discuss the lessons from non-cyber events (such as the 2003 blackouts in North America and Europe, and more recent incidents) to illustrate necessary steps to effectively disabling the delivery of electric services.

As a result of this discussion, attendees will emerge with a more thorough understanding of the number of steps and actions required to overcome existing protections and redundancies in electric environments. Additionally, attendees will learn of potential shortcuts through external events and environmental factors that can enable outsized effects. Overall, this discussion will inform attendees as to the overall complexity of electric systems, and what types of actions are necessary to undermine such systems through cyber means.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## DC - Sunday - 13:00-13:45 PDT

---

**Title:** TBA

**When:** Sunday, Aug 14, 13:00 - 13:45 PDT

**Where:** Caesars Forum - Forum 106-110, 138-139 (Track 2)

**SpeakerBio:** Benny Zeltser , Security Researcher, Intel

No BIO available

### Description:

The SMM is a well-guarded fortress that holds a treasure – an unlimited god mode. We hopped over the walls, fooled the guards, and entered the holy grail of privileges. An attacker running in System Management Mode (SMM) can bypass practically any security mechanism, steal sensitive information, install a bootkit, or even brick the entire platform. We discovered a family of industry wide TOCTOU vulnerabilities in various UEFI implementations affecting more than 8 major vendors making billions of devices vulnerable to our attack. RingHopper leverages peripheral devices that exist on every platform to perform a confused deputy attack. With RingHopper we hop from ring 3 (user-space) into ring -2 (SMM), bypass all mitigations, and gain arbitrary code execution. In our talk, we will deep-dive into this class of vulnerabilities, exploitation method and how it can be prevented. Finally, we will demonstrate a PoC of a full exploitation using RingHopper, hopping from user-space into SMM.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## PT - Monday - 09:00-16:59 PDT

---

**Title:** TCP/IP Deep Dive for Ethical Hackers – Featuring Wireshark

**When:** Monday, Aug 15, 09:00 - 16:59 PDT

**Where:** Caesars Forum

**SpeakerBio:** Chris Greer , Network Analyst & Wireshark Instructor

Chris Greer is a Packet Head. He is a Packet Analyst and Trainer for Packet Pioneer, a Wireshark University partner, and has a passion for digging into the packet-weeds and finding answers to network and cybersecurity problems. Chris has a YouTube channel where he focuses on videos showing how to use Wireshark to examine TCP connections, options, and unusual behaviors, as well as spotting scans, analyzing malware, and other IOC's in the traffic. His approach to training is that if you aren't having fun doing something, you won't retain what you are learning, so he strives to bring as much hands-on and humor to the classroom as possible. Chris remembers what it was like to look at Wireshark for the first time, and knows how complicated packet analysis can be. With that in mind, he has designed an easy-to-follow course that will appeal both to the

beginner and more advanced Packet Person.  
Twitter: [@https://twitter.com/packetpioneer](https://twitter.com/packetpioneer)

## Description:

Latest details, requirements, description, cost:

<https://defcontrainings.myshopify.com/products/chris-greer-tcp-ip-deep-dive-for-hackers-featuring-wireshark>

Training description:

Almost every attack, intrusion, scan, and exfiltration involves the TCP protocol at some point. Whether we are hacking a system and need to better understand how networks/systems are enumerated and IDS's do their thing, or we are defending our domain from a botnet attack, a deep understanding of the TCP protocol will help us do our jobs better and faster. In this course, get ready to go deep into TCP. We're going to rip open pcaps with Wireshark and learn how this protocol really works. Don't worry, there is FAR more to learn past the three-way handshake! We will learn how the MSS works, receive windows, selective acknowledgements, retransmissions, and much, much more! We will examine how TCP scan, OS enumeration, exfiltration, and C2 traffic looks on the wire, and how TCP fields can help us to filter for it fast. This will be an action-packed, hands-on course for Wireshark beginners as well as seasoned pros who want to pick up some new tricks. There is something for all experience levels in this course, although it will be targeted to the early-intermediate cybersecurity professional.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## PT - Tuesday - 09:00-16:59 PDT

---

**Title:** TCP/IP Deep Dive for Ethical Hackers – Featuring Wireshark

**When:** Tuesday, Aug 16, 09:00 - 16:59 PDT

**Where:** Caesars Forum

**SpeakerBio:** Chris Greer , Network Analyst & Wireshark Instructor

Chris Greer is a Packet Head. He is a Packet Analyst and Trainer for Packet Pioneer, a Wireshark University partner, and has a passion for digging into the packet-weeds and finding answers to network and cybersecurity problems. Chris has a YouTube channel where he focuses on videos showing how to use Wireshark to examine TCP connections, options, and unusual behaviors, as well as spotting scans, analyzing malware, and other IOC's in the traffic. His approach to training is that if you aren't having fun doing something, you won't retain what you are learning, so he strives to bring as much hands-on and humor to the classroom as possible. Chris remembers what it was like to look at Wireshark for the first time, and knows how complicated packet analysis can be. With that in mind, he has designed an easy-to-follow course that will appeal both to the beginner and more advanced Packet Person.

Twitter: [@https://twitter.com/packetpioneer](https://twitter.com/packetpioneer)

## Description:

Latest details, requirements, description, cost:

<https://defcontrainings.myshopify.com/products/chris-greer-tcp-ip-deep-dive-for-hackers-featuring-wireshark>

Training description:

Almost every attack, intrusion, scan, and exfiltration involves the TCP protocol at some point. Whether we are hacking a system and need to better understand how networks/systems are enumerated and IDS's do their thing, or we are defending our domain from a botnet attack, a deep understanding of the TCP protocol will help us do our jobs better and faster. In this course, get ready to go deep into TCP. We're going to rip open pcaps with Wireshark and learn how this protocol really works. Don't worry, there is FAR more to learn past the three-way handshake! We will learn how the MSS works, receive windows, selective acknowledgements, retransmissions, and much, much more! We will examine how TCP scan, OS

enumeration, exfiltration, and C2 traffic looks on the wire, and how TCP fields can help us to filter for it fast. This will be an action-packed, hands-on course for Wireshark beginners as well as seasoned pros who want to pick up some new tricks. There is something for all experience levels in this course, although it will be targeted to the early-intermediate cybersecurity professional.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## DC - Friday - 18:00-18:45 PDT

---

**Title:** Tear Down this Zywall: Breaking Open Zyxel Encrypted Firmware

**When:** Friday, Aug 12, 18:00 - 18:45 PDT

**Where:** Caesars Forum - Alliance 301-309, 321 (Track 4)

**SpeakerBio:** Jay Lagorio , Independent Security Researcher

Jay Lagorio, a software engineer and independent security researcher, has been building computers and networks and finding ways to break them nearly his entire life. Being a nerd that likes to dig too far into things spilled over into the real world and he accidentally became a licensed private investigator. Releaser of the occasional tool or writeup on Github, he wishes he had enough time to do all the hacker things and crush griefers in GTA Online every day. He received a B.S. in Computer Science from UMBC and an M. Eng. from the Naval Postgraduate School.

Twitter: [@https://twitter.com/jaylagorio](https://twitter.com/jaylagorio)

### Description:

How do you go bug hunting in devices you own when the manufacturer has slapped some pesky encryption scheme on the firmware? Starting from an encrypted blob of bits and getting to executable code is hard and can be even more frustrating when you already know the bug is there, you just want to see it! Join me on my expedition to access the contents of my Zyxel firewall's firmware using password and hash cracking, hardware and software reverse engineering, and duct taping puzzle pieces together. We'll start with a device and a firmware blob, flail helplessly at the crypto, tear apart the hardware, reverse engineer the software and emulate the platform, and finally identify the decryption routine – ultimately breaking the protection used by the entire product line to decrypt whatever firmware version we want.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## ASV - Friday - 11:00-11:25 PDT

---

**Title:** That's No Moon -- A Look at the Space Threat Environment

**When:** Friday, Aug 12, 11:00 - 11:25 PDT

**Where:** Caesars Forum - Forum 112-117

**SpeakerBio:** Mike Campanelli

Mr. Campanelli currently leads aerospace professional services at Amazon Web Services (AWS). Prior to joining AWS, Mike was the vice president of federal for SpiderOak, leading the creation of OrbitSecure, a zero-trust security protocol for space assets.

### Description:

Outer space has changed, and changed our lives, since the first DEF CON in 1993. This informational talk explores the industry trends we have seen over the last 30 years, growing threats we face to our satellites, and why everyone needs to be informed about the ultimate man-in-the-middle: space.

---

## LPV - Sunday - 14:00-14:20 PDT

---

**Title:** The "Why" of Lock Picking

**When:** Sunday, Aug 14, 14:00 - 14:20 PDT

**Where:** Caesars Forum - Summit 203-204, 235

**SpeakerBio:** Christopher Forte (isaidnocookies)

No BIO available

### Description:

"Why would you possibly need to know how to do that?" and "Couldn't you just break the lock?" are two of the more common questions I get when discussing lock picking or various bypasses. At first glance, many see lock picking as a nefarious and largely unnecessary hobby. But, whether you are a locksport enthusiast, security researcher, emergency responder, or just someone who enjoys puzzles, lock picking can be a constructive—and useful—skill to learn. This talk aims to show how diverse the community is, explore some of the many reasons we engage in this hobby, and try to give some answers as to why we practice lock picking.

---

## WS - Friday - 10:00-13:59 PDT

---

**Title:** The Art of Modern Malware Analysis: Initial Infection Malware, Infrastructure, and C2 Frameworks

**When:** Friday, Aug 12, 10:00 - 13:59 PDT

**Where:** Harrah's - Lake Tahoe

**Speakers:** Aaron Rosenmund, Ryan J Chapman, Josh Stroschein

**SpeakerBio:** Aaron Rosenmund , Threat Emulation and Detection Operator

Aaron Rosenmund is an experienced threat emulation and detection operator. He is the Director of Security Research and Curriculum at Pluralsight, and as the Civilian Red Team Lead for the national DOD exercise Cyber Shield. Part time he serves in the Florida Air National Guard supporting state and federal missions including election support and Operation Noble Eagle (Homeland Defense). An accomplished speaker and trainer, he has over 100 published courses and labs, provided numerous talks and workshops, and continues to support various open source projects. [@arosenmund](http://Www.AaronRosenmund.com) "ironcat"

Twitter: [@https://twitter.com/arosenmund](https://twitter.com/arosenmund)

**SpeakerBio:** Ryan J Chapman , IR Practitioner

Ryan is an experienced IR practitioner, malware analyst, and trainer. He is a Principal IR Consultant for BlackBerry, the lead organizer of CactusCon, a SANS author and trainer, and a Pluralsight author. Ryan strives to imbue comedy into his training and loves being able to teach others while learning from them at the same time. He is a veteran speaker having presented talks and/or workshops at conferences including DefCon, SANS Summits, BSides events, CactusCon, and more. "We must not teach people how to press buttons to get results. We must teach people what happens when these buttons are clicked, such that they fully understand the processes occurring in the background," says Ryan.

**SpeakerBio:** Josh Stroschein , Malware Analyst

Josh is an experienced malware analyst and reverse engineer who has a passion for sharing his knowledge with others. He is

the Director of Training for OISF, where he leads all training activities for the foundation and is also responsible for academic outreach and developing research initiatives. Josh is an accomplished trainer, providing training in the aforementioned subject areas at BlackHat, DerbyCon, Toorcon, Hack-In-The-Box, Suricon and other public and private venues. Josh is an Assistant Professor of Cyber Security at Dakota State University where he teaches malware analysis and reverse engineering, an author on Pluralsight, and a threat researcher for Bromium.

## Description:

Threat actors go to great lengths to bypass enterprise security to deliver malware, avoid detection after the initial intrusion, and maintain persistence to compromise an organization. To achieve this, threat actors employ a wide variety of obfuscation and anti-analysis techniques at each phase of an attack. Often, Malware-as-a-Service (MaaS) is leveraged. In this workshop, you will get hands-on experience with real-world malware and learn how to identify key indicators of compromise (IOCs), apply analysis to enhance security products to protect users and infrastructure, and gain a deeper understanding of malware behavior through reverse engineering.

Our workshop focuses on MaaS samples and their prevalence in attacks. We will break down various MaaS samples and show how they function. We will review attacker-controlled infrastructure to show how Command and Control (C2) features are successful within YOUR (hopefully not YOUR!) environment. We will conclude with an analysis of the world's #1 C2 infrastructure: Cobalt Strike (CS). We will break down the CS infrastructure, show how Malleable C2 profiles function, and show you how to extract and analyze profile configurations from script- and PE-based payloads alike.

Students will be provided with all the lab material used throughout the course in a digital format. This includes all lab material, lab guides, and virtual machines used for training. The material provided will help to ensure that students have the ability to continue learning well after the course ends and maximize the knowledge gained from this course. Whatever isn't covered during the class, or whatever the student wants to focus on later, will be available.

## Materials

Linux/Windows/Mac desktop environment A laptop with the ability to run virtualization software such as VMWare or VirtualBox Access to the system BIOS to enable virtualization, if disabled via the chipset Ability to temporarily disable anti-virus or white-list folders/files associated with lab material A laptop that the attendee is comfortable handling live malware on Enough disk space to store at least two 40 GB VMs, although more VMs may be used 16GB of RAM preferred to run all VMs simultaneously

## Prereq

The primary requirement for this course is a desire to learn and the determination to tackle challenging problems. In addition, having some familiarization with the following topics will help students maximize their time in this course:-  
A general background in Digital Forensics & Incident Response (DFIR) - Familiarity with blue team-oriented tools - An understanding of general networking concepts

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## DC - Saturday - 15:00-15:20 PDT

---

**Title:** The Big Rick: How I Rickrolled My High School District and Got Away With It

**When:** Saturday, Aug 13, 15:00 - 15:20 PDT

**Where:** Caesars Forum - Forum 106-110, 138-139 (Track 2)

**SpeakerBio:** Minh Duong , Student at University of Illinois at Urbana-Champaign

Minh Duong is an undergraduate studying Computer Science at the University of Illinois at Urbana-Champaign. Over the summer, he worked as an application security intern for Trail of Bits, focusing on compositor security and the Wayland protocol. In his free time, he plays CTFs with SIGPwny, UIUC's cybersecurity club. This will be his first time at DEF CON. Twitter: [@https://twitter.com/WhiteHoodHacker](https://twitter.com/WhiteHoodHacker)

## Description:

What happens when you have networked projectors, misconfigured devices, and a bored high school student looking for the perfect senior prank? You get a massive rickroll spanning six high schools and over 11,000 students at one of the largest school districts in suburban Chicago.

This talk will go over the coordination required to execute a hack of this scale and the logistics of commanding a botnet of IoT systems. It will also describe the operational security measures taken so that *you* can evade detection, avoid punishment, and successfully walk at graduation.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## DC - Sunday - 12:00-12:45 PDT

---

**Title:** The Call is Coming From Inside The Cluster: Mistakes that Lead to Whole Cluster Pwnership

**When:** Sunday, Aug 14, 12:00 - 12:45 PDT

**Where:** Caesars Forum - Forum 104-105, 135-136 (Track 1)

**Speakers:** Will Kline, Dagan Henderson

**SpeakerBio:** Will Kline , Senior Principal / Dark Wolf Solutions

Will Kline is a Senior Principal with Dark Wolf Solutions, where he works with different customers to modernize their containerized development environments. He's been working with Linux containers since the pre-Docker days. He has been attending DEF CON since DEF CON 21. He has been coming back almost every year, becoming increasingly involved with the SOHOplessly Broken IoT CTF and the Wireless CTF. At DEF CON 25 his team "Wolf Emoji" took a Black Badge. In his recent work with Dagan, he has been excited to see the intersection between his off-hours hacking fun and real world cloud architecture and SRE work.

**SpeakerBio:** Dagan Henderson , Principal / RAFT

Dagan Henderson is a Principal Engineer at Raft, LLC, where he specializes in Kubernetes platform development. Dagan's interest in hacking dates back to the late 80s when AOL and BBSs were the spots (yep, he hosted a very short lived BBS from his home PC—and it got hacked). His first useful computer program was a DOS BAT on a bootable floppy that removed a very persistent Windows 95 Trojan, which he wrote for the mom-and-pop computer shop he worked at for his first job. While in college, Dagan began working for a medical services provider, and when his acumen with computer systems became well-known, he was asked to evaluate a new electronic medical records system. He was able to identify several information-disclosure vulnerabilities and work with the development team to address them. As his career in software engineering took off, Dagan remained committed to developing secure applications, which is essentially the art of not developing insecure systems, and he remains committed to the practice today. As a 25-year veteran of the industry, Dagan has seen (and made) many, many mistakes. He knows where bodies get buried.

## Description:

Kubernetes has taken the DevOps world by storm, but its rapid uptake has created an ecosystem where many popular solutions for common challenges—storage, release management, observability, etc.—are either somewhat immature or have been “lifted and shifted” to Kubernetes. What critical security smells can pentesters look for when looking at the security of a cluster?

We are going to talk through five different security problems that we have found (and reported, no 0-days here) in popular open-source projects and how you can look for similar vulnerabilities in other projects.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

**Title:** The Chaos of Coding with Language Models

**When:** Friday, Aug 12, 14:00 - 14:50 PDT

**Where:** Caesars Forum - Summit 228->236

**SpeakerBio:** Nick Dorion

No BIO available

### Description:

Language models are being deployed to assist with writing code and explaining code snippets. These transformer-based models have learned patterns and probabilities from large datasets of open source code and human text. A Wired article claims one plugin writes “a remarkable 35 percent of its users’ newly posted code”.

Could these models be a new source of exploits and risky coding practices? What can research in Natural Language Generation tell us about what to expect from our new AI coworkers?

This presentation will cover:

How code explanation models, by reading variable names and comments for context clues, can be tricked to ignore unusual imports and calls to remote servers in their descriptions.

How code generation models may generate different code based on licenses and author names. Others’ research shows these models’ accuracy are highly variable based on “prompt engineering” (example: “I’ve tested this function myself so I know that it’s correct.”).

An adversarial search for comments, prompts, and decoding strategies which would increase the chance of a SQL injection vulnerability in generated code. This helps evaluate if normal user interaction may result in models recommending exploitable coding.

Resources will include a GitHub repo, runnable notebooks, and a form to suggest new prompts for code generation.

---

[Return to Index](#) - Add to



- ics [Calendar file](#)

---

## DC - Saturday - 14:00-14:45 PDT

---

**Title:** The COW (Container On Windows) Who Escaped the Silo

**When:** Saturday, Aug 13, 14:00 - 14:45 PDT

**Where:** Caesars Forum - Academy 401-410, 421 (Track 3)

**SpeakerBio:** Eran Segal , Security research team leader at SafeBreach

Eran Segal is a research team leader, with more than 7 years experience in cyber security research. Over the last three years, he has been researching security projects in SafeBreach Labs, after serving in various security positions in the IDF. He specializes in research on Windows and embedded devices.

### Description:

Virtualization and containers are the foundations of cloud services. Containers should be isolated from the real host’s settings to ensure the security of the host.

In this talk we'll answer these questions: "Are Windows process-isolated containers really isolated?" and "What can an attacker achieve by breaking the isolation?"

Before we jump into the vulnerabilities, we'll explain how Windows isolates the container's processes, filesystem and how the host prevents the container from executing syscalls which can impact the host. Specifically, we'll focus on the isolation implementation of Ntoskrnl using server silos and job objects.

We'll compare Windows containers to Linux containers and describe the differences between their security architectural designs. We'll follow the scenario of an attacker-crafted container running with low privileges. We'll show in multiple ways how to gain privilege escalation inside the container to NT/System. After gaining NT/System permissions, we'll talk about how we escaped the isolation of the container and easily achieved a dump of the entire host's kernel memory from within the container. If the host is configured with a kernel debugger, we can even dump the host's Admin credentials.

We'll finish by demonstrating how an attacker-crafted container with low privileges can read UEFI settings and then set them. Using this technique an attacker can communicate between containers and cause a permanent Denial-of-Service (DoS) to a host with default settings, through the UEFI interface.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## DC - Saturday - 18:00-18:45 PDT

---

**Title:** The CSRF Resurrections! Starring the Unholy Trinity: Service Worker of PWA, SameSite of HTTP Cookie, and Fetch

**When:** Saturday, Aug 13, 18:00 - 18:45 PDT

**Where:** Caesars Forum - Academy 401-410, 421 (Track 3)

**SpeakerBio:** Dongsung Kim , IT-Security Expert, Truesec

Dongsung (Donny) Kim is a security specialist at Truesec || an independent software developer. His software interests vary widely from frontend to DevSecOps, with research interests spanning from reverse engineering to web security. Equipped with both professional and academic experiences, he wants to reconcile two seemingly opposite ideas: understanding user-facing software problems without compromising security.

Twitter: [@https://twitter.com/kid1ng](https://twitter.com/kid1ng)

### Description:

CSRF is (really) dead. SameSite killed it. Browsers protect us. Lax by default!

Sounds a bit too good to be true, doesn't it? We live in a world where browsers get constantly updated with brand new web features and new specifications. The complexity abyss is getting wider and deeper. How do we know web technologies always play perfectly nice with each other? What happens when something slips?

In this talk, I focus on three intertwined web features: HTTP Cookie's SameSite attribute, PWA's Service Worker, and Fetch. I will start by taking a look at how each feature works in detail. Then, I will present how the three combined together allows CSRF to be resurrected, bypassing the SameSite's defense. Also, I will demonstrate how a web developer can easily introduce the vulnerability to their web apps when utilizing popular libraries. I will end the talk by sharing the complex disclosure timeline and the difficulty of patching the vulnerability due to the interconnected nature of web specifications.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## DC - Friday - 11:00-11:45 PDT

---

**Title:** The Dark Tangent & Mkfactor - Welcome to DEF CON & The Making of the DEF CON Badge

**When:** Friday, Aug 12, 11:00 - 11:45 PDT

**Where:** Caesars Forum - Forum 104-105, 135-136 (Track 1)

**Speakers:** The Dark Tangent, Michael Whiteley (Mkfactor), Katie Whiteley (Mkfactor)

**SpeakerBio:** The Dark Tangent , DEF CON

No BIO available

**SpeakerBio:** Michael Whiteley (Mkfactor)

No BIO available

Twitter: [@https://twitter.com/compukidmike](https://twitter.com/compukidmike)

**SpeakerBio:** Katie Whiteley (Mkfactor)

No BIO available

Twitter: [@https://twitter.com/ktjgeekmom](https://twitter.com/ktjgeekmom)

### Description:

The Dark Tangent welcomes you to DEF CON and introduces the DEF CON 30 badge makers Mkfactor, they discuss the labor of love that went into producing the DEF CON 30 Badge.

---

[Return to Index](#) - Add to



- ics [Calendar](#) file

## CPV - Saturday - 14:30-14:59 PDT

---

**Title:** The deadly state of surveillance capitalism in healthcare

**When:** Saturday, Aug 13, 14:30 - 14:59 PDT

**Where:** Flamingo - Vista Ballroom

**Speakers:** Valencia Robinson, Mike Mittelman, Andrea Downing

**SpeakerBio:** Valencia Robinson

Valencia Robinson is a breast cancer survivor, co-founding member of The Light Collective. As a patient advocate with 15 years experience working in the breast cancer community, Valencia is working to advance digital rights for patients and ensure technologies affecting the lives of her community have representation from people of color in the governance and design.

**SpeakerBio:** Mike Mittelman

No BIO available

**SpeakerBio:** Andrea Downing

Andrea Downing is a cancer advocate turned security researcher. Her work has been featured on CNN, Fortune, and The Verge, and has catalyzed an urgent dialogue on national health privacy policy and the need for protections outside of HIPAA. Andrea has co-founded a nonprofit called The Light Collective to work with vulnerable patient groups seeking digital rights and safe spaces for patient support communities on social media.

### Description:

Whether serving up medical misinformation through ads, or brokering patients into predatory startups like Cerebral - patients

going through the trauma of a diagnosis experience harm as they seek knowledge online. This talk will focus on this specific research, and share a broader perspective on the deadly state of surveillance capitalism and ad targeting in healthcare.

In a recent study from researchers at Duke University and the patient privacy-focused group the Light Collective, patient advocates who are active in the hereditary cancer community and cancer support groups on Facebook—including three who are Facebook group admins—downloaded and analyzed their data from the platform's "Off Facebook Activity" feature in September and October. The tool shows what information third parties are sharing with Facebook and its parent company Meta about your activity on other apps and websites. Along with the retail and media sites that typically show up in these reports, the researchers found that several genetic-testing and digital-medicine companies had shared customer information with the social media giant for ad targeting.

This talk will not only share examples of harm, we will talk about what our patient-led collective is doing to help patients take back their privacy.

---

[Return to Index](#) - Add to [!\[\]\(aa7b4139aed126b5e9d846a1e94d68e5\_img.jpg\) Google Calendar](#) - ics [Calendar](#) file

---

## **BTW - Saturday - 13:00-13:59 PDT**

---

**Title:** The DFIR Report Homecoming Parade Panel

**When:** Saturday, Aug 13, 13:00 - 13:59 PDT

**Where:** Virtual - BlueTeam Village - Talks

**Speakers:**Kostas,ICSNick - Nicklas Keijser,Ch33r10,Justin Elze,Jamie Williams,nas\_bench - Nasreddine Bencherchali

### **SpeakerBio:**Kostas

Kostas is a security researcher with many years of experience in the field. Coming from a technical background in incident response, he specializes in intrusion analysis and threat hunting.

Kostas devotes most of his spare time to supporting the information security community by producing free threat intelligence reports as part of the DFIRReport effort, of which he is a member.

### **SpeakerBio:**ICSNick - Nicklas Keijser

Nicklas works as a Threat Research Analyst at the company Truesec, based in Stockholm/Sweden. Here he splits his time picking apart malware from threat actors and as a subject matter expert in Industrial Control System. Also a analyst contributor to The DFIR Report.

### **SpeakerBio:**Ch33r10

Cybersecurity Analyst at a Fortune 500. DSc Cybersecurity, MBA IT Management, 8 x GIAC, and SANS Women's Academy graduate.

### **SpeakerBio:**Justin Elze

Justin is currently serving as CTO/Hacker at TrustedSec and possess a background in red teaming, pentesting, and offensive research.

### **SpeakerBio:**Jamie Williams

Jamie is an adversary emulation engineer for The MITRE Corporation where he works with amazing people on various exciting efforts involving security operations and research, mostly focused on adversary emulation and behavior-based detections. He leads the development of MITRE ATT&CK® for Enterprise and has also led teams that help shape and deliver the “adversary-touch” within MITRE Engenuity ATT&CK Evaluations as well as the Center for Threat-Informed Defense (CTID).

## **SpeakerBio:**nas\_bench - Nasreddine Bencherchali

Avid learner, passionate about all things detection, malware, DFIR, and threat hunting.

### **Description:**

The DFIR Report Homecoming Parade will not discuss normal (BAU) CTI actions, such as searching the logs for hits on the IOCs or entering the IOCs into a Threat Intelligence Platform (TIP) or other alerting platform. Instead, the participants will focus on pivoting, TTPs, and how they would take the contents in the various DFIR Reports to the NEXT LEVEL! When the Panelists respond to the DFIR Reports, they are operating under the assumption that they performed the preliminary analysis and deemed the threat report relevant to their environment. The purpose of this assumption is to decrease the amount of debate on whether or not something is relevant to get to the part of the analysis that involves extracting actionable takeaways.

Follow along as we take the DEF CON Hacker Homecoming theme to the next level with a DFIR Report Homecoming Parade. The panel will provide additional context to various DFIR Reports released in the past year. Pick up some tips and tricks to up your game!

---

[Return to Index](#) - Add to

[Google Calendar](#)

- ics [Calendar](#) file

---

## **ASV - Saturday - 14:30-14:55 PDT**

---

**Title:** The Emerging Space - Cyber Warfare Theatre

**When:** Saturday, Aug 13, 14:30 - 14:55 PDT

**Where:** Caesars Forum - Forum 112-117

### **SpeakerBio:**Eytan Tepper

Eytan Tepper is Visiting Assistant Professor and director of the Space Governance Lab at Indiana University Bloomington. He earned his doctorate from McGill University's Institute of Air and Space Law and pursued a postdoc at NYU Law School. He teaches and leads research on space law & governance.

### **Description:**

A combined space-cyber warfare theatre is emerging to become the primary battlefield in the twenty-first century and the main mode of space warfare. Cyberattacks on critical space-based infrastructure have already been launched by States, criminal organizations, and terrorist groups, and such attacks could even trigger a war. The risks are high, yet current multilateral regimes and most national policies do not address the emerging space-cyber nexus. A new project aims to identify shared norms

---

[Return to Index](#) - Add to

[Google Calendar](#)

- ics [Calendar](#) file

---

## **DC - Saturday - 12:00-12:20 PDT**

---

**Title:** The Evil PLC Attack: Weaponizing PLCs

**When:** Saturday, Aug 13, 12:00 - 12:20 PDT

**Where:** Caesars Forum - Alliance 301-309, 321 (Track 4)

### **SpeakerBio:**Sharon Brizinov , Vulnerability Research Team Lead @ Claroty

Sharon Brizinov leads the vulnerability research at Claroty. Brizinov specializes in vulnerability research, malware analysis, network forensics, and ICS/SCADA security. In addition, Brizinov participated in well-known hacking competitions such as Pwn2Own (2020, 2022), and he holds a DEFCON black-badge for winning the ICS CTF (DEFCON 27).

## Description:

These days, Programmable Logic Controllers (PLC) in an industrial network are a critical attack target, with more exploits being identified every day. But what if the PLC wasn't the prey, but the predator? This presentation demonstrates a novel TTP called the "Evil PLC Attack", where a PLC is weaponized in a way that when an engineer is trying to configure or troubleshoot it, the engineer's machine gets compromised.

We will describe how engineers diagnose PLC issues, write code, and transfer bytecode to PLCs for execution with industrial processes in any number of critical sectors, including electric, water and wastewater, heavy industry, and automotive manufacturing. Then we will describe how we conceptualized, developed, and implemented different techniques to weaponize a PLC in order to achieve code execution on an engineer's machine.

The research resulted in working PoCs against ICS market leaders which fixed all the reported vulnerabilities and remediated the attack vector. Such vendors include Rockwell Automation, Schneider Electric, GE, B&R, Xinje, OVARRO and more.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## BICV - Friday - 10:00-10:30 PDT

---

**Title:** The GACWR Story: Building a Black Owned Cyber Range

**When:** Friday, Aug 12, 10:00 - 10:30 PDT

**Where:** Flamingo - Twilight Ballroom

**Speakers:**Jovonni Pharr,GACWR Team

**SpeakerBio:**Jovonni Pharr

No BIO available

**SpeakerBio:**GACWR Team

No BIO available

**Description:**No Description available

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## DC - Saturday - 12:30-12:50 PDT

---

**Title:** The hitchhacker's guide to iPhone Lightning & JTAG hacking

**When:** Saturday, Aug 13, 12:30 - 12:50 PDT

**Where:** Caesars Forum - Forum 104-105, 135-136 (Track 1)

**SpeakerBio:**stacksmashing , Hacker

stacksmashing is a security researcher with a focus on embedded devices: From hacking payment terminals, crypto-wallets, secure processors or Apple AirTags, he loves to explore embedded & IoT security. On his YouTube channel he attempts to make reverse-engineering & hardware hacking more accessible. He is known for trying to hack everything for under \$5, which is probably related to him living in the stingiest part of Germany.

Twitter: [@https://twitter.com/ghidraninja](https://twitter.com/ghidraninja)

## Description:

Apple's Lightning connector was introduced almost 10 years ago - and under the hood it can be used for much more than just charging an iPhone: Using a proprietary protocol it can also be configured to give access to a serial-console and even expose the JTAG pins of the application processor! So far these hidden debugging features have not been very accessible, and could only be accessed using expensive and difficult to acquire "Kanzi" and "Bonobo" cables. In this talk we introduce the cheap and open-source "Tamarin Cable", bringing Lightning exploration to the masses!

In this talk we are diving deep into the weeds of Apple Lightning: What's "Tristar", "Hydra" and "HiFive"? What's SDQ and IDBUS? And how does it all fit together?

We show how you can analyze Lightning communications, what different types of cables (such as DCSD, Kanzi & co) communicate with the iPhone, and how everything works on the hardware level.

We then show how we developed the "Tamarin Cable": An open-source, super cheap (~\$5 and a sacrificed cable) Lightning explorer that supports sending custom IDBUS & SDQ commands, can access the iPhone's serial-console, and even provides a full JTAG/SWD probe able to debug iPhones.

We also show how we fuzzed Lightning to uncover new commands, and reverse engineer some Lightning details hidden in iOS itself.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## MIV - Friday - 10:00-11:30 PDT

---

**Title:** The hybrid strategies of autocratic states: narrative characteristics of disinformation campaigns in relation to issues of a scientific-health nature

**When:** Friday, Aug 12, 10:00 - 11:30 PDT

**Where:** Caesars Forum - Summit 221->236

**SpeakerBio:** Carlos Galán

Prof. Carlos Galán is a university professor and lawyer specialising in International Relations, Hybrid Threats, Disinformation, Privacy and Cybersecurity. He has worked in several public and private sector institutions, such as the Spanish National Cybersecurity Institute. Author of numerous articles on these topics in various academic, professional and think tanks, he has been part of the European Parliament's research team for the project "Strategic communications as a key factor in countering hybrid threats".

**Description:** No Description available

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## DC - Sunday - 13:00-13:45 PDT

---

**Title:** The Journey From an Isolated Container to Cluster Admin in Service Fabric

**When:** Sunday, Aug 14, 13:00 - 13:45 PDT

**Where:** Caesars Forum - Alliance 301-309, 321 (Track 4)

**SpeakerBio:** Aviv Sasson , Principal security researcher, Palo Alto Networks

Aviv Sasson is a security research team lead in Palo Alto Networks under Prisma Cloud, specializing in cloud, network, and

application security. He started his career in the Israeli intelligence forces and continued to work in the cyber security industry. He is fascinated by container and cloud security and is now working in the Prisma Cloud research team, finding security issues and zero days in the cloud ecosystem.

## Description:

Service Fabric is a scalable and reliable container orchestrator developed by Microsoft. It is widely used in Microsoft Azure as well as in Microsoft's internal production environments as an infrastructure for containerized applications.

Developing a container orchestrator is not an easy task as it involves harnessing many technologies in a complicated and distributed environment. This complexity can ultimately lead to security issues. Such security issues can impose a critical risk since compromising an infrastructure allows attackers to escalate their privileges and take over an entire environment quickly and effectively.

In this session, Aviv will share his research on Service Fabric and his journey of escalating from an isolated container to cluster admin. He will go through researching the code and finding a zero-day vulnerability, explaining his exploitation process in Azure Service Fabric offering while dealing with race conditions and other limitations, and explain how it all allowed him to break out of his container to later gain full control over the underlying Service Fabric cluster.

In the end, he will share his thoughts on security in the cloud and his concerns on cloud multitenancy.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## BICV - Friday - 16:00-16:59 PDT

---

**Title:** The Last Log4Shell Talk You Need

**When:** Friday, Aug 12, 16:00 - 16:59 PDT

**Where:** Virtual - BIC Village

**SpeakerBio:**Ochuan Marshall

No BIO available

**Description:**No Description available

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## LPV - Friday - 12:00-12:30 PDT

---

**Title:** The least secure biometric lock on Earth?

**When:** Friday, Aug 12, 12:00 - 12:30 PDT

**Where:** Caesars Forum - Summit 203-204, 235

**SpeakerBio:**Seth Kintigh

No BIO available

## Description:

I demonstrate how to defeat a biometric padlock via USB with a laptop, or with your bare hands, or maybe even with a Defcon badge.

While flipping through products a biometric lock caught my attention. It mentioned a back-up “Morse code” feature for unlocking it -- a series of 6 short or long presses, suggesting there were only 64 possible keys. Surely it couldn’t be that easy... But wait, there’s more! It had another backup unlock feature: a USB port and an app that can unlock it with a PIN, with a default PIN set for bonus stupidity. I had a feeling this was just the tip of the terrible-security-iceberg.

I will demonstrate how to defeat this lock with some simple tools, with just your bare hands, and with a USB attack.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## CPV - Friday - 14:30-14:59 PDT

---

**Title:** The Multiverse of Madness: Navigating the 50-State Approach to Privacy and Security

**When:** Friday, Aug 12, 14:30 - 14:59 PDT

**Where:** Flamingo - Vista Ballroom

### **SpeakerBio:** Anthony Hendricks

Anthony Hendricks is a legal problem solver and litigator at Crowe & Dunlevy in its Oklahoma City office. At Crowe & Dunlevy, Hendricks chairs the firm’s Cybersecurity and Data Privacy Practice Group. He guides clients facing sensitive criminal, cybersecurity, banking, and environmental compliance issues. Hendricks teaches a cybersecurity law class and an information privacy class 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.

### **Description:**

States have been taking the lead to address privacy. Last year, multiple states introduced or strengthened their privacy laws, and in 2022 several states are primed to do the same. But these new laws raise concerns for both the public and companies. Some of these new privacy laws don’t match public perception and worries related to privacy. In addition, these new laws are being crafted by state legislators that few people voted for. Voter turnout in local elections is historically low, and the people who vote in these elections don’t reflect the demographics of their districts. Even still, these new laws can be great for consumers. But it often leaves companies, especially small and medium-sized ones, struggling to address this new normal and leaving communities with regulations that they aren’t prepared for. Companies working nationally or even regionally must navigate multiple state privacy demands. This presentation will provide an update on these new laws and how they compare to public perception of privacy. Next, we will examine their impact on privacy and security, outline some common characteristics of these laws, and provide tips for companies to be privacy compliant. Finally, we talk about ways the public can shape these new laws.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## DC - Friday - 11:00-11:45 PDT

---

**Title:** The PACMAN Attack: Breaking PAC on the Apple M1 with Hardware Attacks

**When:** Friday, Aug 12, 11:00 - 11:45 PDT

**Where:** Caesars Forum - Academy 401-410, 421 (Track 3)

### **SpeakerBio:** Joseph Ravichandran , First year PhD Student working with Dr. Mengjia Yan at MIT

Joseph Ravichandran is a PhD student in computer architecture studying microarchitectural security at MIT. His work includes microarchitectural and memory safety attacks and attack modeling. He plays CTF with SIGPwny. This is his first DEF CON talk.

Twitter: [@https://twitter.com/0xjprx](https://twitter.com/0xjprx)

## Description:

What do you get when you cross pointer authentication with microarchitectural side channels?

The PACMAN attack is a new attack technique that can bruteforce the pointer authentication code (PAC) for an arbitrary kernel pointer without causing any crashes using microarchitectural side channels. We demonstrate the PACMAN attack against the Apple M1 CPU.

[Return to Index](#) - Add to



- ics [Calendar file](#)

## WS - Thursday - 10:00-13:59 PDT

**Title:** The Purple Malware Development Approach

**When:** Thursday, Aug 11, 10:00 - 13:59 PDT

**Where:** Harrah's - Elko

**Speakers:** Olaf Hartong, Mauricio Velazco

**SpeakerBio:** Olaf Hartong , Defensive Specialist

Olaf Hartong is a Defensive Specialist and security researcher at FalconForce. He specializes 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 WWHF, 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.

**SpeakerBio:** Mauricio Velazco , Principal Threat Research Engineer

Mauricio Velazco (@mvelazco) is a Principal Threat Research Engineer at Splunk. Prior to Splunk, he led the Threat Management team at a Fortune 500 organization. Mauricio has presented and hosted workshops at conferences like Defcon, BlackHat, Derbycon, BSides and SANS. His main areas of focus include detection engineering, threat hunting and adversary simulation.

Twitter: [@https://twitter.com/mvelazco](https://twitter.com/mvelazco)

## Description:

This workshop merges offensive and defensive lab exercises to provide attendees hands-on experience on custom malware development as well as live malware analysis and response. The workshop has a total of 5 hands-on exercises and each contains a Red and a Blue section. In the Red section attendees write custom payloads using C# and C++ with different techniques to obtain a reverse shell on a Windows victim endpoint. In the Blue section attendees investigate the infection by reviewing events and logs using open source static and dynamic malware analysis tools like CFFExplorer, Pe-Studio, dnSpy, Process Explorer, Process Monitor, Sysmon, Frida, Velociraptor, etc..

## Materials

Laptop with virtualization software. A Windows virtual machine A Kali Linux Virtual Machine.

## Prereq

Beginner to intermediate programming/scripting skills. Prior experience with C# helps but not required. Beginner static and dynamic malware analysis skills.

[Return to Index](#) - Add to



- ics [Calendar file](#)

## SKY - Friday - 12:10-12:30 PDT

---

**Title:** The Richest Phisherman in Colombia

**When:** Friday, Aug 12, 12:10 - 12:30 PDT

**Where:** LINQ - BLOQ

**Speakers:**Matt Mosley,Nick Ascoli

### **SpeakerBio:**Matt Mosley

Matt Mosley is a security professional with 30+ years experience in various technical and executive roles, former UNIX sysadmin and software engineer, and reformed grey hat hacker who wears his original “I miss crime” shirt proudly. In his current role as Chief Product Officer and CISO of security startup PIXM, Matt guides the company’s product and security strategy and manages several functional teams. Matt has held the CISSP, CISM and CISA credentials since the mid 90s and has spoken on security topics many times over the years, from large audiences at RSA to local ISSA meetings. Matt believes that security starts with the basics that most companies fail to get right, and would be happy to debate the merits of the principles in the orange book vs your need for the latest XDR/SOAR/ABCDXYZ product. He is still waiting for the right opportunity to avenge his team’s finals loss in Hacker Jeopardy during Defcon 5.

### **SpeakerBio:**Nick Ascoli

Nick Ascoli is the founder and CEO of Foretrace, an External Attack Surface Management (EASM) solution. Prior to starting Foretrace, Nick was a Cyber Research Scientist and Consultant with Security Risk Advisors and has published several open-source tools including pdblaster and TALR. Nick has been a speaker at Blackhat Arsenal, SANS, and B-Sides conferences on SIEM, Recon, and UEBA topics.

Twitter: [@https://twitter.com/kcin418](https://twitter.com/kcin418)

### **Description:**

Adversaries have increasingly been leveraging completely legitimate 3rd party web hosting products to circumvent traditional domain reputation analysis engines, and successfully get their phishing pages in front of their victims. Using these third party services also offers them a great opportunity to limit the exposure of their own infrastructure, offering a great OPSEC advantage. However, in one investigation, a few breadcrumbs left in the adversaries code led us down a rabbit hole to slowly uncovering the person behind what is perhaps the largest Facebook credential harvesting campaign ever investigated (over 100 million potentially impacted at the time of this submission).

In this talk, we will follow the breadcrumb trail left by a threat actor, demonstrating how we pieced together the shocking scale of their credential harvesting and malversating operation. From comments in their code, to their various online identities, to accessing their infrastructure - we will walk through our investigation into a wanted Colombian Cyber Criminal.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## LPV - Friday - 14:00-14:59 PDT

---

**Title:** The Right Way To Do Wrong: Physical security secrets of criminals and professionals alike

**When:** Friday, Aug 12, 14:00 - 14:59 PDT

**Where:** Caesars Forum - Summit 203-204, 235

### **SpeakerBio:**Patrick McNeil

No BIO available

### **Description:**

In 1905 Harry Houdini wrote his first book entitled “The Right Way to Do Wrong” wherein he divulged the lockpicking and

other trade secrets of criminals. People make assumptions about how schemes work and believe them to be complicated, yet in many cases the insider knows how simple they are. Most people assume that besides tailgating and social engineering, real break-ins (or physical security testing) are all about picking locks. However, the secret is that on physical pentests it's typically unnecessary to do that! Some physical controls have known bypasses, and some building contractors (or even locksmiths) don't implement things correctly. Just like Houdini, I'll be divulging the simple tricks of the trade employed by both criminals and professional physical pentesters to bypass physical controls without using picks. You may be shocked and amazed by what you see, and once you leave you'll be an insider too - seeing insecurity everywhere!

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## **AIV - Saturday - 14:00-14:50 PDT**

---

**Title:** The Use of AI/ML in Offensive Security Operations

**When:** Saturday, Aug 13, 14:00 - 14:50 PDT

**Where:** Caesars Forum - Summit 228->236

### **Description:**

The Red Team Village and the AI Village will host a panel from different industry experts to discuss the use of artificial intelligence and machine learning in offensive security operations. More details coming soon!

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## **DL - Friday - 10:00-11:55 PDT**

---

**Title:** TheAllCommander

**When:** Friday, Aug 12, 10:00 - 11:55 PDT

**Where:** Caesars Forum - Accord Boardroom

### **SpeakerBio:**Matthew Handy

Matt Handy completed his BS in Computer Science at the University of Maryland, College Park (UMD) in 2010, and MS in CyberSecurity at Johns Hopkins in 2014. He has worked for NASA's Goddard Space Flight Center doing satellite ground systems development since 2009. He has specialized in secure software systems development and has helped to develop several missions over the course of his career. In his off time, he enjoys doing independent security research and creating tools like TheAllCommander to help make a more secure cyber world.

### **Description:**

TheAllCommander is an open-source tool which offers red teams and blue teams a framework to rapidly prototype and model malware communications, as well as associated client-side indicators of compromise. The framework provides a structured, documented, and object-oriented API for both the client and server, allowing anyone to quickly implement a novel communications protocol between a simulated malware daemon and its command and control server. For Blue Teamers, this allows rapid modeling of emerging threats and comprehensive testing in a controlled manner to develop reliable detection models. For Red Teamers, this framework allows rapid iteration and development of new protocols and communications schemes with an easy to use Python interface. The framework has many tools or techniques used by red teams built in, such as a SOCKS5 proxy, which then use the implemented communication scheme. This allows comprehensive testing of the detection and functional capability of the communication scheme, allowing for efficient design and development choices to be made before committing to production tool development. To facilitate this goal, TheAllCommander includes a Java based command and control server with a simple API to allow new plug-ins for server-side control. There is a python-based emulation client, which can be easily extended using the API to allow new client side communications code. Several reference

implementations for covert malware communication are provided to allow out-of-the-box modeling, including emulated client browser HTTPS traffic, DNS queries, and email traffic. The tool chain includes support for several common Red Team tactics, such as Remote Desktop tunneling and FODHelper UAC bypass. This implementation effectively generates both client side and network traffic indicators of compromise.

Audience: Offense, Defense

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## SKY - Saturday - 11:40-12:30 PDT

---

**Title:** This one time, at this Hospital, I got Ransomware

**When:** Saturday, Aug 13, 11:40 - 12:30 PDT

**Where:** LINQ - BLOQ

### **SpeakerBio:**Eirick Luraas

Eirick spends his days discovering and mitigating vulnerabilities, occasionally doing Incident Response, and once in a while tracking down bad actors. Sometimes he gets to compromise systems to show Executives that Hospitals are horribly insecure.

Eirick earned a Master's Degree in Cybersecurity, and he has spoken several times about the dangers technology creates in healthcare. Eirick helps bring awareness of the risks we are unknowingly taking every time we visit a Hospital and works every day to reduce those dangers.

Eirick grew up in Montana and lived in Panama during his military service. He bounced around a few states in the US. He recently relocated to Tucson, Az where he is rediscovering his passion for photography. You can follow Eirick on twitter @tyercel.

Twitter: [@https://twitter.com/tyercel](https://twitter.com/tyercel)

### **Description:**

Most people don't know how Hospitals go through a ransomware incident. This lack of understanding creates a false sense of security for the places we rely on to help us when we are at our most vulnerable. This talk will describe what happened during a ransomware incident at a small midwestern hospital.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## BTW - Saturday - 11:00-11:59 PDT

---

**Title:** Threat Hunt Trilogy: A Beast in the Shadow!

**When:** Saturday, Aug 13, 11:00 - 11:59 PDT

**Where:** Virtual - BlueTeam Village - Talks

### **SpeakerBio:**Dr. Meisam Eslahi

Meisam is a technical cybersecurity practitioner with solid expertise in providing strategies and technical directions, building new service/business lines, diverse teams, and capabilities. He has over 20 years of experience in information technology, with 16 years dedicated to cybersecurity in leadership and technical roles leading a wide range of services for multi-national clients mainly in Red Teaming, Threat Hunting, DFIR, Cyber Drill, Compromise Assessment, and Penetration Testing. He is also a security researcher [MITRE D3FEND contributor], blogger [cybermeisam.medium.com], mentor, and speaker in many global

events and conferences such as Defcon, BSidesSG, and NASSCOM.

## Description:

Although file-less threats may require some sort of files to operate or indirectly use them in some part of their lifecycle (e.g., infection chain), their malicious activities are conducted only in the memory. The adversaries misuse the trusted applications or native utilities such as PowerShell and WMI to download and load malicious codes directly into memory and execute them without touching the hard disk.

The newly discovered file-less threat campaign utilizes an innovative technique for the first time to store and hide its shellcode in the Windows event logs, which will be loaded and used by a dropper in the last stage of the infection lifecycle. To put it simply, the file-less threat could be a nightmare for blue teams and threat hunters.

This technical talk will briefly explain the different categories of file-less threats; however, as the title suggests, the focus of this trilogy will be a file-less threat hunt via three different approaches as follows:

- System Live Analysis: A few techniques such as running processes and lineage analysis, command-line Strings, masquerading and obfuscation, and port to process mapping will be used to look for the file-less threat traces on a live active system.
- Memory Forensics: This is one of the most exciting parts as it dives into the main territory of file-less threats and examines PowerShell execution, process tree, hierarchy, and handles to look for any potential signs of threats.
- Network Packet Investigation: Network conversations, malicious HTTP requests, files transferred, and adversaries' commands will be extracted from network packets (i.e., a sample PCAP file) to hunt the file-less threat used in the previous parts.

Finally, a comparative review discusses the advantages and disadvantages of the above techniques. All the three approaches will be conducted using open-source and free tools, native operating system commands, and built-in utilities. The threat hunt hypothesis and educated guesses will be formulated based on the industrial test cases provided by MITRE ATT&CK, D3fend, and CAR [Cyber Analytics Repository].

File-less threats operate in silence and stealth, enabling adversaries to bypass automated cybersecurity, lurk in our digital wonderland, and avoid standard detections. They are hidden beasts in shadow! This technical talk will briefly explain the different types of file-less threats and the importance of threat hunting to combat them. A Windows-based file-less threat will also be hunted via the live system, memory, and network packet analysis, followed by a comparative discussion about each method's capabilities. The threat hunts' hypotheses used in this presentation are practical, and all will be mapped with MITRE knowledge bases.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## BICV - Saturday - 15:00-15:30 PDT

---

**Title:** Threat hunting? Ain't nobody got time for that...

**When:** Saturday, Aug 13, 15:00 - 15:30 PDT

**Where:** Virtual - BIC Village

**SpeakerBio:**Nick Gobern

No BIO available

**Description:**No Description available

---

## SOC - Thursday - 18:00-01:59 PDT

---

**Title:** Thursday Opening Party - Entertainment

**When:** Thursday, Aug 11, 18:00 - 01:59 PDT

**Where:** Caesars Forum - Forum 120-123, 129, 137

**Speakers:**FuzzyNop,Archwisp,DJ St3rling,Dr. McGrew,Magician Kody Hildebrand,NPC Collective,TRIODE,Ytcracker

**SpeakerBio:**FuzzyNop

No BIO available

**SpeakerBio:**Archwisp

No BIO available

**SpeakerBio:**DJ St3rling

No BIO available

**SpeakerBio:**Dr. McGrew

No BIO available

**SpeakerBio:**Magician Kody Hildebrand

No BIO available

**SpeakerBio:**NPC Collective

No BIO available

**SpeakerBio:**TRIODE

No BIO available

**SpeakerBio:**Ytcracker

No BIO available

### Description:

18:00 - 19:00: Hildebrand Magic

19:00 - 20:00: NPC Collective

20:00 - 21:00: Archwisp

21:00 - 22:00: Dr. McGrew

22:00 - 23:00: DJ St3rling

23:00 - 00:00: ytcracker

**00:00 - 01:00: TRIODE**

01:00 - 02:00: FuzzyNop

---

## MIV - Saturday - 10:00-10:45 PDT

---

**Title:** Tools for Fighting Disinformation

**When:** Saturday, Aug 13, 10:00 - 10:45 PDT

**Where:** Caesars Forum - Summit 221->236

**SpeakerBio:** Preslav Nakov

Dr. Preslav Nakov leads the Tanbih mega-project (<http://tanbih.qcri.org/>), developed in collaboration with MIT. The project's aim is to build a news aggregator that limits the effect of fake news, propaganda and media bias by helping users step out of their bubble and achieve a healthy news diet. He is also the lead-PI of a QCRI-MIT collaboration project on Arabic Speech and Language Processing for Cross-Language Information Search and Fact Verification, and he was a co-PI of another QCRI-MIT collaboration project on Speech and Language Processing for Arabic (2013-2016). Dr. Nakov is Secretary of ACL SIGSLAV and also a Secretary of ACL SIGSLAV.

**Description:** No Description available

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## DC - Saturday - 15:30-16:15 PDT

---

**Title:** Tor: Darknet Opsec By a Veteran Darknet Vendor & the Hackers Mentality

**When:** Saturday, Aug 13, 15:30 - 16:15 PDT

**Where:** Caesars Forum - Forum 106-110, 138-139 (Track 2)

**SpeakerBio:** Sam Bent , KS LLC

Former admin and co-founder on Dread Forum (Darknet), staff on multiple Darknet sites, Darknet vendor: 2happytimes2, lockpicker, hacker, hak5 enthusiast, haxme.org admin (Clearnet), Sam Bent spends his days writing technical manuals and doing graphics (using all Adobe Products) for the company he works for, while also doing federal prison consulting on the side. He is a certificated paralegal. Runs his blog where he does federal prison consulting, is currently about to publish a book on compassionate release for federal prisoners, and runs multiple youtube channels. He is a student in college,

He has been in the scene for almost 20 years. He has written multiple guides and published numerous whitepapers and how-to's on hacking, including one article written in combination with r4tdance (of #suidrewt) published on packetstomsecurity called A Newbies Guide To The Underground Volume 2. Sam Bent's former handles include killab, 2happytimes, 2happytimes2, and most recently, DoingFedTime.

Twitter: [@https://twitter.com/DoingFedTime](https://twitter.com/DoingFedTime)

**Description:**

The hacking subculture's closest relative is that of the Darknet. Both have knowledgeable people, many of whom are highly proficient with technology and wish to remain somewhat anonymous. They are both composed of a vast amount of introverts and abide by the same first rule: "Don't get caught."

Over the past decade, there have been many DEF CON talks that have discussed topics related to Tor and the Darknet. Having an IT, Infosec, and hacking background, the goal is to present a unique perspective from a hacker turned Darknet Vendor, who then learned about the law and—using metaphorical privilege escalation and social engineering—got himself out of federal prison after a year and a half by acting as his own lawyer.

The focus of this talk will surround operational security policies that a skilled Darknet Market Vendor (DMV) implements to avoid compromising their identity. We will look at tactics used by Law Enforcement and common attacks prevalent on the

Darknet, ranging from linguistic analysis and United States Postal Inspector operations all the way to correlation attacks and utilizing long-range wifi antennas to avoid detection as a failsafe.

By focusing less on the basics of Tor and more on how insiders operate within it, we will uncover what it takes to navigate this ever-evolving landscape with clever OpSec.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## CPV - Saturday - 16:15-16:59 PDT

---

**Title:** Toto, I've a feeling we're not on a VPN anymore

**When:** Saturday, Aug 13, 16:15 - 16:59 PDT

**Where:** Flamingo - Vista Ballroom

**SpeakerBio:** Jonathan Tomek

Jonathan Tomek serves as VP of Research and Development with Digital Envoy, parent company of Digital Element. His expertise is in threat intelligence, network forensics, incident handling, and malware analysis.

He is a former Marine, a co-founder of THOTCON (Chicago's biggest hacking event), and CTF creator. You may remember him from such films as "That one Sake Bomb" or "Hackers Go West! Part Deux" You can find him on Twitter: @sakebomb

Twitter: [@https://twitter.com/sakebomb](https://twitter.com/sakebomb)

### Description:

You are savvy enough to have a virtual private network aka VPN. Maybe you did a bit of research and bought one that lets you be “anonymous” and lets you stream your favorite streaming service from anywhere while you travel.

How much do you know about or trust your VPN provider? Have you considered that your VPN provider could be doing things you didn't expect? Let's look at consumer VPNs, free VPNs, even VPNs that pay you!

After analyzing hundreds of VPNs, their service offerings, and their code, you will have a deeper understanding of what actually is happening behind the scenes. Could you be supporting malware? Maybe something worse? This may be a talk you don't want to hear, but you will come out of it with a better understanding of the world that says it is here to protect you.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## SOC - Thursday - 16:00-21:59 PDT

---

**Title:** Toxic BBQ

**When:** Thursday, Aug 11, 16:00 - 21:59 PDT

**Where:** Other/See Description

### Description:

16:00- 22:00 Thursday, Off-site at Sunset Park, Pavilion F, (36.0636, -115.1178)

The humans of Vegas invite you to the 16th in-carne-tion of this unofficial welcome party. Go AFK 4 BBQ off-Strip and make us the first stop on your DC30 reunion tour. Burgers and dogs are provided; attendees are encouraged to pitch in with more food, drinks, volunteer labor, rides, and everything that makes this cookout something to remember.

Grab flyers from an Info Booth after Linecon, check out <https://www.toxicbbq.org> for the history of this event, and watch #ToxicBBQ on Twitter for the latest news.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## DC - Friday - 14:30-15:15 PDT

---

**Title:** Trace me if you can: Bypassing Linux Syscall Tracing

**When:** Friday, Aug 12, 14:30 - 15:15 PDT

**Where:** Caesars Forum - Alliance 301-309, 321 (Track 4)

**Speakers:** Rex Guo, Junyuan Zeng

### **SpeakerBio:** Rex Guo , Principal Engineer

Rex Guo works as a Principal Engineer at Lacework where he leads data-driven cloud security product development, detection efficacy roadmap and research on new attack vectors in the cloud. Previously, he was the Head of Research at Confluera where he led the research and development of the cloud XDR product which offers real-time attack narratives. Before that, he was an Engineering Manager at Cisco Tetration where his team bootstrapped the cloud workload protection product deployed on millions of workloads. Before that, Rex worked at Intel Security and Qualcomm. In these positions, he worked on application security, infrastructure security, malware analysis, and mobile/IoT security. Most notably, he led the Intel team to secure millions of iPhones which had Intel cellular modems inside. He has presented at Blackhat and Defcon multiple times. He has 30+ patents and publications. He received a PhD from New York University.

Twitter: [@https://twitter.com/Xiaofei\\_REX](https://twitter.com/Xiaofei_REX)

### **SpeakerBio:** Junyuan Zeng , Senior Software Engineer, LinkedIn.com

Junyuan Zeng is Senior Software Engineer at LinkedIn. Before LinkedIn, he was Staff Security Architect at JD.com where he designed and architected container security monitoring solutions. Before that he was Staff Software Engineer for mobile payment security at Samsung and a security researcher at FireEye where he worked on mobile malware analysis. He has spoken multiple times at Blackhat and Defcon. He has published in ACM CCS, USENIX ATC, and other top academic conferences. He obtained his PhD in Computer Science from The University of Texas at Dallas.

### **Description:**

In this talk, we will present novel vulnerabilities and exploitation techniques that reliably bypass Linux syscall tracing. A user mode program does not need any special privileges or capabilities to reliably avoid system call tracing detections by exploiting these vulnerabilities. The exploits work even when seccomp, SELinux, and AppArmor are enforced.

Advanced security monitoring solutions on Linux VMs and containers offer system call monitoring to effectively detect attack behaviors. Linux system calls can be monitored by kernel tracing technologies such as tracepoint, kprobe, ptrace, etc. These technologies intercept system calls at different places in the system call execution. These monitoring solutions can be deployed on cloud compute instances such as AWS EC2, Fargate, EKS, and the corresponding services from other cloud providers.

We comprehensively analyzed the Time-of-check-to-time-of-use (TOCTOU) issues in the Linux kernel syscall tracing framework and showed that these issues can be reliably exploited to bypass syscall tracing. Our exploits manipulate different system interactions that can impact the execution time of a syscall. We demonstrated that significant syscall execution delays can be introduced to make TOCTOU bypass reliable even when seccomp, SELinux, and AppArmor are enforced. Compared to the phantom attacks in DEFCON 29, the new exploit primitives we use do not require precise timing control or synchronization.

We will demonstrate our bypass for Falco on Linux VMs/containers and GKE. We will also demonstrate bypass for pdig on AWS Fargate. In addition, we will demonstrate exploitation techniques for syscall enter and explain the reason why certain configurations are difficult to reliably exploit. Finally, we will summarize exploitable TOCTOU scenarios and discuss

potential mitigations in various cloud computing environments.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## DC - Saturday - 12:00-12:20 PDT

---

**Title:** Tracking Military Ghost Helicopters over our Nation's Capital

**When:** Saturday, Aug 13, 12:00 - 12:20 PDT

**Where:** Caesars Forum - Forum 106-110, 138-139 (Track 2)

**SpeakerBio:** Andrew Logan

Andrew Logan is an audio engineer, videographer and DJ based in Washington, D.C. He is an aerospace and radio nerd, and a fierce defender of the First Amendment.

Twitter: [@https://twitter.com/HelicoptersofDC](https://twitter.com/HelicoptersofDC)

**Description:**

There's a running joke around Washington D.C. that the "State Bird" is the helicopter. Yet 96% of helicopter noise complaints from 2018-2021 went unattributed: D.C. Residents can not tell a news helicopter from a black hawk. Flight tracking sites remove flights as a paid service to aircraft owners and government agencies; even in the best case these sites do not receive tracking information from most military helicopters due to a Code of Federal Regulations exemption for "sensitive government mission for national defense, homeland security, intelligence or law enforcement." This makes an enormous amount of helicopter flights untraceable even for the FAA and leaves residents in the dark.

What if we could help residents identify helicopters? What if we could crowd source helicopter tracking? What if we could collect images to identify helicopters using computer vision? What if we could make aircraft radio as accessible as reading a map? What if we could make spotting helicopters a game that appeals to the competitive spirit of Washingtonians? And what if we could do all of this... on Twitter?

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## MIV - Friday - 16:00-16:59 PDT

---

**Title:** Tracking Scams and Disinformation by Hacking Link Shorteners

**When:** Friday, Aug 12, 16:00 - 16:59 PDT

**Where:** Caesars Forum - Summit 221->236

**Speakers:** Justin Rhinehart, Sam Curry

**SpeakerBio:** Justin Rhinehart

Justin Rhinehart is a Senior Security Analyst on the Cosmos team at Bishop Fox. In his spare time, he enjoys doing security research and bug bounty with his friends, as well as creating security-related content. Additionally, he has lectured on cybersecurity at the University of Guadalajara, been featured in both Dark Reading and Ars Technica, volunteered in the Virtual and Western Regions of the Collegiate Cyber Defense Competition, and has served on the board of three non-profit organizations focused on giving back to his local community.

**SpeakerBio:** Sam Curry

No BIO available

**Description:**No Description available

[Return to Index](#) - Add to



- ics [Calendar](#) file

## DC - Saturday - 16:00-16:45 PDT

**Title:** Trailer Shouting: Talking PLC4TRUCKS Remotely with an SDR

**When:** Saturday, Aug 13, 16:00 - 16:45 PDT

**Where:** Caesars Forum - Forum 104-105, 135-136 (Track 1)

**Speakers:**Ben Gardiner,Chris Poore

**SpeakerBio:**Ben Gardiner , Senior Cybersecurity Research Engineer, National Motor Freight Traffic Association Inc., Ben Gardiner is a Senior Cybersecurity Research Engineer contractor at the National Motor Freight Traffic Association, Inc. (NMFTA) specializing in hardware and low-level software security. Prior to joining the NMFTA team in 2019, Gardiner held security assurance and reversing roles at a global corporation, as well as worked in embedded software and systems engineering roles at several organizations. He is a DEF CON Hardware Hacking Village and Car Hacking Village volunteer. He also participates in and contributes to working groups in SAE and ATA TMC.

**SpeakerBio:**Chris Poore , Senior Reverse Engineer, Assured Information Security

Chris Poore is a Senior Reverse Engineer at Assured Information Security in Rome, NY. He has expertise discovering vulnerabilities in wireless systems, gaining access to systems via RF, reverse engineering RF protocols, forensically testing cybersecurity systems, and administering RF collection events. He has experience writing code for software-defined radios and GNU Radio to reverse-engineer RF communication protocols and perform sophisticated attacks. Chris is excitable when working with the community to draw out ideas and takes advantage of networking opportunities with both humans and computers.

### Description:

Ben Gardiner, Chris Poore and other security researchers have been analyzing signals and performing research against trailers and Power Line Communication for multiple years. This year the team was able to disclose two vulnerabilities focused on the ability to remotely inject RF messages onto the powerline and in turn send un-authenticated messages to the brake controller over the link. The team will discuss the details of PLC4TRUCKS, identify what led to this research and the discovery of the vulnerabilities, and then highlight the details of the SDR and software used to perform the attack. The talk will conclude with the demonstration of a remotely induced brake controller solenoid test using an FL2K and the release of the GNU radio block used to perform the test to the community to promote further research in the area.

[Return to Index](#) - Add to



- ics [Calendar](#) file

## DC - Saturday - 12:30-13:15 PDT

**Title:** UFOs, Alien Life, and the Least Untruthful Things I Can Say.

**When:** Saturday, Aug 13, 12:30 - 13:15 PDT

**Where:** Caesars Forum - Forum 106-110, 138-139 (Track 2)

**SpeakerBio:**Richard Thieme , ThiemeWorks

Richard Thieme is an author/professional speaker who addresses “the human in the machine,” technology-related security and intelligence issues as they come home to our humanity. He has published hundreds of articles, dozens of stories, seven books, and delivered hundreds of speeches, including for NSA, FBI, the Secret Service, etc. He spoke in 2021 at Def Con for the 25th

year and has keynoted security conferences in 15 countries. His latest book about an intelligence professional, "Mobius: A Memoir," is a novel receiving over-the-top reviews.  
Twitter: [@https://twitter.com/neuralcowboy](https://twitter.com/neuralcowboy)

## Description:

I have explored the subject of UFOs seriously and in depth and detail for 44 years. I have worked with some of the best and brightest in the "invisible college" to do academic research and reach conclusions based on the evidence. I contributed to the celebrated history, "UFOs and Government: A Historical Inquiry," the gold standard for historical research into the subject now in over 100 university libraries. This talk more than updates the latest government statements on the subject--it is the most complete, honest, and forthright presentation I can make. I will tell the most truth I can, based on data and evidence. As an NSA analyst told me, "Richard, they are here. They're here."

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## DL - Saturday - 12:00-13:55 PDT

---

**Title:** unblob - towards efficient firmware extraction

**When:** Saturday, Aug 13, 12:00 - 13:55 PDT

**Where:** Caesars Forum - Caucus Boardroom

**Speakers:** Quentin Kaiser, Florian Lukavsky

### **SpeakerBio:** Quentin Kaiser

Quentin Kaiser is an ex-penetration tester who turned binary analysis nerd. He's currently working as a security researcher at the ONEKEY Research Lab, where he focuses on binary exploitation of embedded devices and bug finding automation within large firmware.

### **SpeakerBio:** Florian Lukavsky

Florian Lukavsky started his hacker career in early ages, bypassing parental control systems. Since then, he has reported numerous zero-day vulnerabilities responsibly to software vendors and has conducted hundreds of pentests and security reviews of IoT devices as a CREST certified, ethical hacker. Today, Florian Lukavsky aid organizations with IoT security automation as CTO of ONEKEY, the leading European platform for automated security analyses of IoT firmware.

## Description:

Unblob is a command line extraction tool to obtain content from any kind of binary blob. It has been initially developed for the sound and safe extraction of arbitrary firmware images. It has been built as a modular framework where anyone can develop and submit new format handlers and extractors. Its public version already supports a large number of filesystems, archive, and compression formats: <https://github.com/onekey-sec/unblob>

Audience: Reverse Engineers, Embedded Security

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## MIV - Friday - 11:30-13:30 PDT

---

**Title:** Uncovering multi-platform misinformation campaigns with Information Tracer

**When:** Friday, Aug 12, 11:30 - 13:30 PDT

**Where:** Caesars Forum - Summit 221->236

## **SpeakerBio:**Zhouhan Chen

Zhouhan Chen received his Ph.D. in Data Science from NYU. He wrote his Ph.D. thesis with a focus on how misinformation spreads across multiple platforms. He currently building two projects with his Ph.D. advisors: Information Tracer (<https://informationtracer.com/>), a platform to detect (mis)disinformation across social media platforms, and Malware Discoverer (<https://zhouhanc.github.io/malware-discoverer/>), a proactive system to discover malicious URL redirection campaigns. His systems are used by researchers, journalists and security analysts.

## **Description:**No Description available

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## **CLV - Sunday - 10:00-10:40 PDT**

---

**Title:** Understanding, Abusing and Monitoring AWS AppStream 2.0

**When:** Sunday, Aug 14, 10:00 - 10:40 PDT

**Where:** Flamingo - Scenic Ballroom

### **SpeakerBio:**Rodrigo Montoro

Rodrigo "Sp0oKeR" Montoro has more than 20 years of experience in Information Technology and Computer Security. Most of his career worked with open source security software (firewalls, IDS, IPS, HIDS, log management, endpoint monitoring), incident detection & response, and Cloud Security. Currently, he is a Senior Threat Detection Engineer at Tempest Security. Before that, he worked as Cloud Researcher at Tenchi Security, Head of Research and Development at Apura Cyber Intelligence, SOC/Researcher at Clavis, Senior Security Administrator at Sucuri, Researcher at Spiderlabs. Author of 2 patented technologies involving innovation in the detection field. One is related to discovering malicious digital documents. The second one is in how to analyze malicious HTTP traffic. Rodrigo has spoken at several open-source and security conferences (OWASP AppSec, SANS (DFIR ,SIEM Summit and CloudSecNext), Defcon Cloud Village, Toorcon (USA), H2HC (S o Paulo and Mexico), SecTor (Canada - 5x), CNASI, SOURCE Boston & Seattle, ZonCon (Amazon Internal Conference), Blackhat Brazil, BSides (Las Vegas e S o Paulo)).

Twitter: [@https://twitter.com/spookerlabs](https://twitter.com/spookerlabs)

### **Description:**

Amazon Web Services (AWS) is a complex ecosystem with hundreds of different services. In the case of a security breach or compromised credentials, attackers look for ways to abuse the customer's configuration of services with their compromised credentials, as the credentials are often granted more IAM permissions than is usually needed. Most research to date has focused on the core AWS services, such as , S3, EC2, IAM, CodeBuild, Lambda, KMS, etc. In our research, we present our analysis on a previously overlooked attack surface that is ripe for abuse in the wrong hands - an AWS Service called Amazon AppStream 2.0. Amazon AppStream 2.0 is a fully managed desktop service that provides users with instant access to their desktop applications from anywhere. Using AppStream 2.0, you can add your desktop applications to a virtual machine and share access to the VM by sharing a link - without requiring any credentials, you can share an image (an attack toolset) with a target account without needing any approval from the other side or attach some privileged role to an image and get those credentials.

In this talk, you'll learn about how AppStream works, how misconfigurations and excessive IAM permissions can be abused to compromise your AWS environment and allow attackers to control your entire AWS account. We'll cover tactics such as persistence, lateral movement, exfiltration, social engineering, and privilege escalation. We will also cover the key indicators of compromise for security incidents in AppStream and how to prevent these abuse cases, showing how excessive privileges without great monitoring could become a nightmare in your Cloud Security posture, making possible attackers control your AWS account.

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## CLV - Saturday - 13:40-14:20 PDT

---

**Title:** us-east-1 Shuffle: Lateral Movement and other Creative Steps Attackers Take in AWS Cloud Environments and how to detect them

**When:** Saturday, Aug 13, 13:40 - 14:20 PDT

**Where:** Flamingo - Scenic Ballroom

### **SpeakerBio:** Felipe Espósito

Felipe Espósito also known as Pr0teus, graduated in Information Technology at UNICAMP and has a master's degree in Systems and Computing Engineering from COPPE-UFRJ, both among the top technology universities in Brazil. He has over ten years of experience in information security and IT, with an emphasis on security monitoring, networking, data visualization, threat hunting, and Cloud Security. Over the last years he has worked as a Security Researcher for Tenchi Security, a Startup focused in secure the cloud, he also presented at respected conferences such as Hackers 2 Hackers Conference, BHACK, BSides (Las Vegas and São Paulo), FISL, Latinoware, SecTor, SANS SIEM Summit, and Defcon's CloudSec Village.

Twitter: [@https://twitter.com/Pr0teusBR](https://twitter.com/Pr0teusBR)

### **Description:**

Attackers do not always land close to their objectives (data to steal). Consequently, they often need to move laterally to accomplish their goals. That is also the case in cloud environments, where most organizations are increasingly storing their most valuable data. So as a defender, understanding the possibilities of lateral movements in the cloud is a must.

Because the control plane APIs are exposed and well documented, attackers can move between networks and AWS accounts by assuming roles, pivoting, and escalating privileges. It is also possible for attackers to move relatively easily from the data plane to the control plane and vice-versa.

In this talk, we are going to explore how attackers can leverage AWS Control and Data Planes to move laterally and achieve their objectives. We will explore some scenarios that we discovered with our clients and how we approached the problem. We will also share a tool we created to help us visualize and understand those paths.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## HHV - Friday - 10:00-10:45 PDT

---

**Title:** Uwb Security Primer: Rise Of A Dusty Protocol

**When:** Friday, Aug 12, 10:00 - 10:45 PDT

**Where:** Flamingo - Exec Conf Ctr - Red Rock VI, VII, VII

### **SpeakerBio:** Göktay Kaykusuz

Göktay Kaykusuz has more than five years of experience in various cyber security fields and is currently a Security Engineer at eyeo GmbH. Previously he worked as a Security Engineer at Jotform Inc. and did freelance/consultancy work before that. Göktay also has Bachelor's Degree in Computer Engineering, a Master's Degree in Information Security, and OSCP/OSCE certifications. He also designed a custom badge to wear, just for DEFCON 30.

Göktay also likes riding cruisers/choppers, smoking churchwardens, and robotics in general. He also dislikes nature to a degree (especially bugs/spiders) and would welcome the warm embrace of Cult Mechanicus if given the opportunity.

## Description:

UWB has been available for nearly 20 years now but never took off the way it was meant to. Every use-case designed or considered for UWB had been taken over by other protocols such as Bluetooth, and like the VR tech, UWB did not become a widespread way of communication for a long time.

During this talk, we will look at the standards, current applications, and possible attack vectors alongside the available hardware that we can utilize to discover these vectors. This session will be a primer for anyone interested in the current UWB landscape and will try to provide the basis for security research.

---

[Return to Index](#) - Add to



- ics [Calendar](#) file

---

## DL - Friday - 10:00-11:55 PDT

---

**Title:** Vajra - Your Weapon To Cloud

**When:** Friday, Aug 12, 10:00 - 11:55 PDT

**Where:** Caesars Forum - Committee Boardroom

**SpeakerBio:** Raunak Parmar

Raunak Parmar works as a Security Consultant. Web/Cloud security, source code review, scripting, and development are some of his interests. Also, familiar with PHP, NodeJs, Python, Ruby, and Java. He is OSWE certified and the author of Vajra and 365-Stealer.

## Description:

Vajra (Your Weapon to Cloud) is a framework capable of validating the cloud security posture of the target environment. In Indian mythology, the word Vajra refers to the Weapon of God Indra (God of Thunder and Storms). Because it is cloud-connected, it is an ideal name for the tool. Vajra supports multi-cloud environments and a variety of attack and enumeration strategies for both AWS and Azure. It features an intuitive web-based user interface built with the Python Flask module for a better user experience. The primary focus of this tool is to have different attacking and enumerating techniques all in one place with web UI interfaces so that it can be accessed anywhere by just hosting it on your server. The following modules are currently available:

- Azure - Attacking 1. OAuth Based Phishing (Illicit Consent Grant Attack) - Exfiltrate Data - Enumerate Environment - Deploy Backdoors - Send mails/Create Rules 2. Password Spray 3. Password Brute Force - Enumeration 1. Users 2. Subdomain 3. Azure Ad 4. Azure Services - Specific Service 1. Storage Accounts
- AWS - Enumeration 1. IAM Enumeration 2. S3 Scanner - Misconfiguration

Audience: Security Professional Cloud Engineer

---

[Return to Index](#) - Add to



- ics [Calendar](#) file

---

## SOC - Saturday - 21:00-01:59 PDT

---

**Title:** VETCON

**When:** Saturday, Aug 13, 21:00 - 01:59 PDT

**Where:** Caesars Forum - Forum 106, 139

## Description:

Co-founded in 2018 by Jim McMurry and William Kimble, the founders of Milton Security and Cyber Defense Technologies, respectively, the VETCON conference is the official Veteran event of the DEFCON Hacker Conference. VETCON, through

its Discord server and in person events, we connect and support veterans in the Information Security field. The event is open to all DEFCON attendees with a focus on military veterans.

VETCON Is a Conference for Veterans, Run by Veterans, During the Largest Hacker Conference, DEFCON

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## DC - Sunday - 10:00-14:59 PDT

---

**Title:** Village Areas Open (Generally)

**When:** Sunday, Aug 14, 10:00 - 14:59 PDT

**Where:** Other/See Description

### Description:

These are the *general* operating hours for villages, across all locations. Refer to each village's location to see their specific hours or activities.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## DC - Saturday - 10:00-17:59 PDT

---

**Title:** Village Areas Open (Generally)

**When:** Saturday, Aug 13, 10:00 - 17:59 PDT

**Where:** Other/See Description

### Description:

These are the *general* operating hours for villages, across all locations. Refer to each village's location to see their specific hours or activities.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## DC - Friday - 10:00-17:59 PDT

---

**Title:** Village Areas Open (Generally)

**When:** Friday, Aug 12, 10:00 - 17:59 PDT

**Where:** Other/See Description

### Description:

These are the *general* operating hours for villages, across all locations. Refer to each village's location to see their specific hours or activities.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

**Title:** Voldrakus: Using Consent String Steganography to Exfiltrate Browser Fingerprinting Data

**When:** Sunday, Aug 14, 11:00 - 11:30 PDT

**Where:** Flamingo - Vista Ballroom

### **SpeakerBio:**Kaileigh McCrea

Kaileigh is a Privacy Engineer at Confiant, where she researches violations of privacy regulations and user rights in ad tech, and builds tools to detect them, and consumes huge amounts of cookies. Before joining Confiant she was a software engineer at Swing Left and Vote Forward where she helped volunteers send over 18 million GOTV letters in the 2020 General Election. Her background includes software engineering, comedy writing, and politics, and when she's not working, she is usually reading excessive amounts and hanging out with her dog.

### **Description:**

The IAB TCF consent string is an encoded data structure which is supposed to hold information about a user's privacy preferences to communicate them to would be trackers on a page to ensure GDPR compliance. Consent string abuse is serious, but using the consent string itself to smuggle out the payload from invasive data collection is a new level of audacity. Walk through a real case of consent string steganography we caught operating at a massive scale.

---

[Return to Index](#) - Add to



- ics [Calendar](#) file

## SKY - Saturday - 12:45-13:35 PDT

---

**Title:** Voter Targeting, Location Data, and You

**When:** Saturday, Aug 13, 12:45 - 13:35 PDT

**Where:** LINQ - BLOQ

### **SpeakerBio:**l0ngrange

No BIO available

Twitter: [@https://twitter.com/l0ngrange](https://twitter.com/l0ngrange)

### **Description:**

Voter targeting firms use “microtargeting” to help campaigns target individual voters to get them to go vote (or stay home and not vote). Data brokers buy your location data from scummy apps and resell it in bulk, claiming the data is anonymized. Now, location data brokers are giving these voter targeting firms unfettered access to the non-anonymized location data of hundreds of millions of voters to further this chicanery.

---

[Return to Index](#) - Add to



- ics [Calendar](#) file

## ASV - Saturday - 14:00-14:25 PDT

---

**Title:** Vulnerability Assessment of a Satellite Simulator

**When:** Saturday, Aug 13, 14:00 - 14:25 PDT

**Where:** Caesars Forum - Forum 112-117

### **SpeakerBio:**Henry Haswell

Mr. Haswell is a Research Engineer at Southwest Research Institute (SwRI), supporting projects focusing on embedded software development and cyber security. He has performed penetration testing on satellite systems, automotive components, embedded systems, and automotive applications.

## Description:

This research performed a vulnerability assessment of a realistic satellite system, demonstrated some of these vulnerabilities on a high-fidelity satellite simulator, and proposed security solutions for discovered vulnerabilities. If the attacks successfully performed against our satellite simulator were to be performed against a real satellite, it would have significantly harmful effects, including loss of data confidentiality, reduced functionality, or a total loss of access to the satellite

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## DL - Friday - 12:00-13:55 PDT

---

**Title:** Wakanda Land

**When:** Friday, Aug 12, 12:00 - 13:55 PDT

**Where:** Caesars Forum - Caucus Boardroom

**SpeakerBio:** Stephen Kofi Asamoah

Stephen Kofi Asamoah (q0phi80) is an Offensive Security professional, with over fifteen (15) years of experience running Offensive Security operations. Some of his previous places of employment include Ernst & Young, PwC and IBM X-Force Red. Currently as a Snr. Manager of Offensive Cybersecurity Operations, he runs an Enterprise's Offensive Security programs and manages a team of Offensive Security Operators.

## Description:

Wakanda Land is a Cyber Range deployment tool that uses terraform for automating the process of deploying an Adversarial Simulation lab infrastructure for practicing various offensive attacks. This project inherits from other people's work in the Cybersecurity Community, to which I have added some additional sprinkles to their work from my other research. The tool deploys the following for the lab infrastructure (of course, more assets can be added): -Two Subnets -Guacamole Server --This provides dashboard access to --Kali GUI and Windows RDP instances The Kali GUI, Windows RDP and the user accounts used to log into these instances are already backed into the deployment process --To log into the Guacamole dashboard with the guacadmin account, you need to SSH into the Guacamole server using the public IP address (which is displayed after the deployment is complete) and then change into the guacamole directory and then type cat .env for the password (the guacadmin password is randomly generated and saved as an environment variable) -Windows Domain Controller for the Child Domain (first.local) -Windows Domain Controller for the Parent Domain (second.local) -Windows Server in the Child Domain -Windows 10 workstation in the Child Domain -Kali Machine - a directory called toolz is created on this box and Covenant C2 is downloaded into that folder, so its just a matter of running Covenant once you are authenticated into Kali -Debian Server serving as Web Server 1 - OWASP's Juice Shop deployed via Docker -Debian Server serving as Web Server 2 - Vulnerable web apps

Audience: Offensive - Defensive - Any Cybersecurity enthusiasts

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar file](#)

---

## DC - Friday - 13:30-13:50 PDT

---

**Title:** Weaponizing Windows Syscalls as Modern, 32-bit Shellcode

**When:** Friday, Aug 12, 13:30 - 13:50 PDT

**Where:** Caesars Forum - Academy 401-410, 421 (Track 3)

**Speakers:**Tarek Abdelmotaleb,Dr. Bramwell Brizendine

**SpeakerBio:**Tarek Abdelmotaleb , Security Researcher, VERONA Labs

Tarek Abdelmotaleb is a security researcher at VERONA Labs, and he is a graduate student at Dakota State University, who will soon graduate with a MS in Computer Science. Tarek specializes in malware development, software exploitation, reverse engineering, and malware analysis. Tarek recently published an IEEE paper that provides a new way for finding the base address of kernel32, making it possible to do shellcode without needing to make use of walking the Process Environment Block (PEB).

**SpeakerBio:**Dr. Bramwell Brizendine

Dr. Bramwell Brizendine completed his Ph.D. in Cyber Operations recently, where he did his dissertation on Jump-Oriented Programming, a hitherto, seldom-studied and poorly understood subset of code-reused attacks. Bramwell developed a fully featured tool that helps facilitate JOP exploit development, the JOP ROCKET. Bramwell is the Director of the Vulnerability and Exploitation Research for Offensive and Novel Attacks (VERONA Lab), specializing in vulnerability research, software exploitation, software security assessments, and the development of new, cutting-edge tools and techniques with respect to software exploitation and malware analysis. Bramwell also teaches undergraduate, graduate, and doctoral level courses in software exploitation, reverse engineering, malware analysis, and offensive security. Bramwell teaches the development of modern Windows shellcode from scratch in various courses. Bramwell is a PI on an NSA grant to develop a shellcode analysis framework. Bramwell has been a speaker at many top security conferences, such as DEF CON, Black Hat Asia, Hack in the Box Amsterdam, Hack, and more.

### Description:

While much knowledge exists on using syscalls for red team efforts, information on writing original shellcode with syscalls so in modern x86 is sparse and lacking. Our reverse engineering efforts, however, have revealed the necessary steps to take to successfully perform syscalls in shellcode, both for Windows 7 and 10, as there are some significant differences.

In this talk, we will embark upon a journey that will show the process of reverse engineering how Windows syscalls work in both Windows 7 and 10, while focusing predominately on the latter. With this necessary foundation, we will explore the process of effectively utilizing syscalls inside shellcode. We will explore the special steps that must be taken to set up syscalls – steps that may not be required to do equivalent actions with WinAPI functions.

This talk will feature various demonstrations of syscalls in x86 shellcode.

---

[Return to Index](#) - Add to



- ics [Calendar](#) file

---

## CLV - Friday - 12:30-13:10 PDT

---

**Title:** Weather Proofing GCP Defaults

**When:** Friday, Aug 12, 12:30 - 13:10 PDT

**Where:** Flamingo - Scenic Ballroom

**SpeakerBio:**Shannon McHale

Shannon McHale, Associate Consultant at Mandiant, has spent her first year in the security industry focused on Red- Teaming cloud environments and recently passed the Google Cloud Certified Professional Cloud Security Engineer (PCSE) exam. As one of Mandiant's Google Cloud Platform (GCP) Subject Matter Experts (SME), she works hard on enhancing and delivering the GCP Penetration Test methodology. This is her first DefCon, but she has presented at ShmooCon and the Women in Cybersecurity (WiCyS) conferences, while simultaneously obtaining her Bachelor's of Science in Computing Security from Rochester Institute of Technology.

Twitter: [@https://twitter.com/\\_shannon\\_mchale](https://twitter.com/_shannon_mchale)

## Description:

Default Google Cloud Platform (GCP) configurations include open ports, high numbers of excessive permissions, limited logging, and credential expiration dates, which security professionals would typically never let happen. But, we cannot expect users in GCP environments to know and prioritize the most secure option for each setting when they configure a resource. This inadvertently leads to unsafe environments that attackers can leverage.

In this talk, we will review the 'dangerous defaults' of GCP and how they can be abused by attackers. We'll also provide specific policies cloud architects and cloud administrators should implement to stop their users from deploying default configurations and outline how to set up policies that reduce decision fatigue on their users. The goal is for cloud architects, engineers, and Blue Teamers to implement what they see in this talk and scale their environment to be significantly more secure. It will also give my fellow Red Teamers a list of items to check for during their assessments to help organizations further harden their environments.

---

[Return to Index](#) - Add to



- ics [Calendar file](#)

---

## MIV - Saturday - 14:45-15:15 PDT

---

**Title:** Web Monetization: A privacy-preserving and open way to earn from Content

**When:** Saturday, Aug 13, 14:45 - 15:15 PDT

**Where:** Caesars Forum - Summit 221->236

**SpeakerBio:** Uchi Uchibeke

No BIO available

**Description:** No Description available

---

[Return to Index](#) - Add to



- ics [Calendar file](#)

---

## BTW - Saturday - 11:00-14:59 PDT

---

**Title:** Web Shell Hunting

**When:** Saturday, Aug 13, 11:00 - 14:59 PDT

**Where:** Virtual - BlueTeam Village - Workshops

**SpeakerBio:** Joe Schottman

Joe Schottman has worn most hats in IT and Security, ranging from application development to DevOps to offensive and defensive security. The nexus of this experience is research into Web Shells. He's spoken and given training on topics such as Purple Teams, API security, Web Shells, Web Threat Hunting, and more at AppSec Village at DEF CON, OWASP Global, SANS Summits, various BSides, Circle City Con, and other events.

## Description:

This workshop will provide the basics of what web shells are, how they are typically used, defensive strategies to prevent them, and ways they can be detected in different layers of security. The detection layers that will be covered are antivirus/endpoint protection, file integrity monitoring, file system analysis, log analysis, network traffic analysis, and endpoint anomaly detection.

Participants will be provided with a virtual machine image that they could both exploit with web shells and perform threat hunting on.

The breakdown is roughly this:

60-80 minutes - what web shells are, what they're used for, ways they can be detected 20 minutes - overview of my perspective on what web threat hunting is and how it varies from conventional threat hunting (TLDR - if you're on the internet, you're always going to be attacked so it's not a matter of picking up an unknown threat so much as filtering through evidence to determine if an attack is actually dangerous) 90+ minutes - hands-on exercises covering various ways to detect web shells such as file integrity monitoring, deobfuscation, YARA, dirty words, time stomping, etc. And then exploiting a vulnerable application and uploading a Web Shell and showing how it can be used to plunder data.

Web Shells are malicious web applications used for remote access. They've been used in many of the recent prominent breaches/vulnerabilities including Equifax, SolarWinds, and ProxyLogon and are used by APTs and other threats. With ProxyLogon, the FBI was authorized to remove them from victim machines.

This session will help you avoid telling your employer that the FBI is now doing volunteer admin work by teaching you about Web Shells, how to hunt for them, and doing hands-on hunting in a VM. A little groundwork goes a long way and this class will show what to do.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## SKY - Saturday - 10:35-11:25 PDT

---

**Title:** What your stolen identity did on its CoViD vacation

**When:** Saturday, Aug 13, 10:35 - 11:25 PDT

**Where:** LINQ - BLOQ

**SpeakerBio:**Judge Taylor

The Hon., Rev., Dr. Taylor, Esq., J.D. (because fucking titles.. am I right?), Judge, Firearms Law Attorney, drafter of fine old fashioned legislation, righter of wrongs, and fucking cripple; is annoyed, loud, and as funny as your worst enemy's heart attack; is an expert in what the government ought not to do.. but the government keeps doing anyway.

Twitter: [@https://twitter.com/mingheemouse](https://twitter.com/mingheemouse)

**Description:**

A judge tells you how and why Billions of U.S. taxpayer dollars were stolen by domestic and foreign hackers and scammers, with the help of the U.S. government. If you saw an attorney annihilate a bunch of hostile watermelons with a \$19 homemade gun and homemade ammunition at the 2017 SkyTalks.. Well he's a Judge now.. and he has to deal with unemployment appeals from identity theft victims who are wondering why they mysteriously have to pay back unemployment programs in 6 different States. Oh.. and GUNS.. he talks about GUNS too..

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## BICV - Saturday - 10:00-10:45 PDT

---

**Title:** When The "IT" Hits The Fan, Stick To the Plan

**When:** Saturday, Aug 13, 10:00 - 10:45 PDT

**Where:** Flamingo - Twilight Ballroom

**SpeakerBio:**Levone Campbell

No BIO available

**Description:**No Description available

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## BHV - Friday - 11:00-11:59 PDT

---

**Title:** Where there's a kiosk, there's an escape

**When:** Friday, Aug 12, 11:00 - 11:59 PDT

**Where:** Flamingo - Laughlin I,II,III

**SpeakerBio:**Michael Aguilar (v3ga)

Michael (v3ga) is a Principia Consultant within Secureworks Adversary group covering a wide range of testing capabilities inclusive of Red Team simulations, Network Penetration Testing, hardware and Medical Devices. v3ga currently has 4 CVE's pertaining to medical device vulnerabilities.

Twitter: [@https://twitter.com/v3ga\\_hax](https://twitter.com/v3ga_hax)

**Description:**No Description available

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## CLV - Saturday - 10:40-11:20 PDT

---

**Title:** Who Contains the “Serverless” Containers?

**When:** Saturday, Aug 13, 10:40 - 11:20 PDT

**Where:** Flamingo - Scenic Ballroom

**SpeakerBio:**Daniel Prizmant

Daniel started out his career developing hacks for video games and soon became a professional in the information security field. He is an expert in anything related to reverse engineering, vulnerability research, and the development of fuzzers and other research tools. To this day Daniel is passionate about reverse engineering video games at his leisure. Daniel holds a Bachelor of Computer Science from Ben Gurion University.

Twitter: [@https://twitter.com/pushrsp](https://twitter.com/pushrsp)

**Description:**

What is Serverless? Serverless computing is a cloud computing execution model in which the cloud provider allocates machine resources on-demand, taking care of the servers on behalf of their customers.

"Serverless" is a misnomer in the sense that servers are still used by cloud service providers to execute code for developers.

How does Serverless work? Where is this Serverless code executed? Who's in charge of securing it? There are many questions surrounding the topic of Serverless computing.

In this talk, I will present to you my research on Serverless Functions. I will show you how I managed to break the serverless interface barrier and what is hidden behind it. I will also show you how I managed to break out of the container that was

supposed to contain my possibly malicious code and get to the underlying host.

I will start by explaining what is Serverless and the idea behind it. I will show some prime examples of what Serverless is supposed to be used for. I will continue with a break out of the cloud provider interface to show you the infrastructure of the machine, the server of the serverless function, that is actually running the code.

After that, I will begin walking you through my research and journey from the point of view of an attacker. I will show you how I discovered the image that the container was running and the steps I took to reverse engineer it.

From there, the path to an elevation of privileges to root to escaping the container was short. I will walk you through a very old but useful exploit I used to escalate my containerized root access to a full-on container breakout. To finish the talk, I will discuss some of the mitigations that were in place in this instance by the cloud provider, and why they were critical in this scenario.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## SOC - Saturday - 22:00-23:59 PDT

---

**Title:** Whose Slide Is It Anyway? (WSIIA)

**When:** Saturday, Aug 13, 22:00 - 23:59 PDT

**Where:** Caesars Forum - Alliance 301-309, 321 (Track 4)

### Description:

It's our sixth year but since we had to be virtual last year this will be our 5 YEAR ANNIVERSARY show of "Whose Slide Is It Anyway"?! We're an unholy union of improv comedy, hacking and slide deck sado-masochism.

Our team of slide monkeys will create 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.

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. Oh, and prizes. Lots and lots of prizes.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## DC - Saturday - 16:30-17:15 PDT

---

**Title:** Why did you lose the last PS5 restock to a bot Top-performing app-hackers business modules, architecture, and techniques

**When:** Saturday, Aug 13, 16:30 - 17:15 PDT

**Where:** Caesars Forum - Forum 106-110, 138-139 (Track 2)

**SpeakerBio:** Arik , Threat Intelligence Researcher, PerimeterX

For the last four years, Arik spent most of his time on darknet and deep web marketplaces, hunting threat intelligence and interacting with hackers under 64 identities.

As a Threat Intelligence Researcher in PerimeterX, Arik trades cracking tools and executes multiple honeypot operations that

provide valuable intelligence about web-automated attacks and their actors. Arik's research focuses primarily on retail bots, NTF bots, and account take-over vectors: brute-force and cookie info stealers.

Previously, Arik worked as the first Threat Researcher at BrightData (Formerly Luminati networks). Between 2018 and 2020, Arik was responsible for investigating, limiting, and blocking 50K\$/Month+ clients that misused the Brightdata residential proxy network for cyberattacks. Analyzing the proxy server logs exposed him to complex fraud operations - from the attacker's perspective.

As a proxy network gatekeeper, he investigated and enticed app-sec hackers to share their pain points, hacking mindsets, and techniques, information He leverages in his current role at PerimeterX when researching relevant attack groups and increasing the accuracy of the company's products.

## Description:

The rise of the machines.

Whenever you are buying online, especially if it's a limited stock item, you are competing against Bots and lose miserably. Even when you are asleep, there's a 14% chance that a bot trying to log into one of the 200+ digital accounts you own.

Your mom called to say someone from her bank ask for 4 digit SMS? It was an OTP bot.

Malicious automation is here to stay as it serves tens of thousands of hackers and retail scalpers and drives billions of dollars worth of marketplaces.

During my talk, we will deep dive into the most fascinating architecture, business modules, and techniques top-performing of account crackers and retail bots use to maximize their success rate and revenue.

---

[Return to Index](#) - Add to



- ics [Calendar file](#)

---

## WS - Saturday - 10:00-13:59 PDT

---

**Title:** Windows Defence Evasion and Fortification Primitives

**When:** Saturday, Aug 13, 10:00 - 13:59 PDT

**Where:** Harrah's - Reno

**Speakers:**Rohan Durve,Paul Laîné

**SpeakerBio:**Rohan Durve , Senior Security Consultant

Rohan (@Decode141) is a Senior Consultant at Mandiant with a primary interest in attack simulation. Rohan is most interested Windows and Active Directory assessments but is also involved delivering offensive security training and capability development. Rohan's presented at conferences such BlackHat, BSides London and BSides LV in the past.

Twitter: [@https://twitter.com/Decode141](https://twitter.com/Decode141)

**SpeakerBio:**Paul Laîné , Senior Security Consultant

Paul L. (@amOnsec) is a Senior Consultant at Mandiant. Paul works in R&D to improve Simulated Attack (SA) capabilities. With a strong interest in Microsoft Windows system and low-level programming, and x86 Instruction Set Architecture (ISA). Paul specialises in the development of malware and tools for SA operations. Some of his work is publicly available on GitHub and discussed on his Twitter profile.

Twitter: [@https://twitter.com/amOnsec](https://twitter.com/amOnsec)

## Description:

The Windows Defence Evasion and Fortification Primitives workshop will walk candidates through adapting initial access,

code execution, credential access and lateral movement TTPs against commonly encountered defences (such as Anti-Virus, Endpoint Detection Tooling and Windows Credential Guard). Candidates will be challenged to think critically and expand their classroom knowledge of vulnerabilities against limitations in defensive technologies on Windows 10, 11, Server 2016 and Server 2019 systems.

## Agenda:

- Connectivity and Setup Tests
- Initial Endpoint Compromise and Code Execution

- Discussing common defensive challenges
  - ◆ AV
  - ◆ Application control
  - ◆ Process relationship
  - ◆ Process flow using Attack Surface Reduction Rules
  - ◆ AMSI - Initial Access
  - ◆ DLL Hijacking/Proxying
    - ◊ Identifying common issues
    - ◊ Creating DLLs - Living out-of-land
  - ◆ SOCKS Proxy
    - ◊ Unmanaged code
    - ◊ Managed code - In-process/In-memory unmanaged code execution
  - ◆ Leveraging C2 capabilities
  - ◆ Injection - Credential Access
  - ◆ Interrogating Browsers
    - ◊ Information gathering
    - ◊ Extracting secrets
  - ◆ LSA
    - ◊ Running Mimikatz/Keeko
    - ◊ What's a protected process?
    - ◊ In-memory patching using
    - ◊ Discussing other methods
    - ◊ Credential Guard
    - ◊ Remote Desktop Credential Guard
    - ◊ Effects of EDR
    - ◊ Kerberos
      - Session 0
      - Code Injection
      - TGS Exports - Lateral Movement
    - SMB
  - ◆ Artefacts
  - ◆ Customisation
    - ◊ Service
    - ◊ Named pipe
      - Alternatives (WinRM/RDP)

- ◆ Artefacts
- ◆ SOCKS Proxy

### Materials

Laptop capable of outbound SSH/RDP to our labs.

### Prereq

Workshop candidates should familiarise themselves with common tooling (such as a C2, PowerShell, MS Build, Rubeus and Keeko) and have experience using common Windows protocols (such as SMB and RDP). Suggested exercises and labs for this will be sent to registered candidates prior to the workshop.

## DC - Friday - 16:00-16:45 PDT

---

**Title:** Wireless Keystroke Injection (WKI) via Bluetooth Low Energy (BLE)

**When:** Friday, Aug 12, 16:00 - 16:45 PDT

**Where:** Caesars Forum - Academy 401-410, 421 (Track 3)

**Speakers:** Fernando Perera, Jose Pico

**SpeakerBio:** Fernando Perera , Security Analyst at LAYAKK

Fernando Perera has been a Security Engineer at LAYAKK for 5 years, where he collaborates on RedTeam projects, development of security tools and software analysis. He has previously presented at RootedCON Satelite VLC 2016 and 2019, among other security events.

**SpeakerBio:** Jose Pico , Founder at LAYAKK

Jose Pico is co-founder and senior security analyst in LAYAKK. Apart from carrying out red team activities and product security evaluations, he is a researcher in wireless communications security. In this field he has published books, articles and research in the form of talks in top events, both in Spain and worldwide. He is also an appointed member of the Ad hoc Working Group on the candidate European Union 5G Cybersecurity Certification Scheme (EU5G AHWG).

### Description:

"We present a Microsoft Windows vulnerability that allows a remote attacker to impersonate a Bluetooth Low Energy (BLE) keyboard and perform Wireless Key Injection (WKI) on its behalf. It can occur after a legitimate BLE keyboard automatically closes its connection because of inactivity. In that situation, an attacker can impersonate it and wirelessly send keys. In this talk we will demonstrate the attack live and we will explain the theoretical basis behind it and the process that led us to discover the vulnerability. We will also release the tool that allows to reproduce the attack and we will detail how to use it."

---

## DL - Saturday - 14:00-15:55 PDT

---

**Title:** Xavier Memory Analysis Framework

**When:** Saturday, Aug 13, 14:00 - 15:55 PDT

**Where:** Caesars Forum - Society Boardroom

**SpeakerBio:** Solomon Sonya , Director of Cyber Operations Training

Solomon Sonya (@Carpenter1010) is the Director of Cyber Operations Training at a large organization. He has a background in software development, malware analysis, covert channels, steganography, distributed computing, computer hacking, information protection paradigms, and cyber warfare. He received his Undergraduate Degree in Computer Science and has Master's degrees in Computer Science and Information System Engineering. Before becoming Director of Cyber Operations Training, he was a university Computer Science Assistant Professor of Computer Science and Research Director. Solomon's current research includes computer system exploitation, cyber threat intelligence, digital forensics, and data protection.

Solomon's previous keynote and conference engagements include: BlackHat USA, SecTor Canada, Hack in Paris, France, HackCon Norway, ICSIS – Toronto, ICORES Italy, BruCon Belgium, CyberCentral – Prague and Slovakia, Hack.Lu Luxembourg, Shmoocon DC, BotConf - France, DerbyCon Kentucky, SkyDogCon Tennessee, HackerHalted Georgia, Day-Con Ohio, and TakeDownCon Connecticut, Maryland, and Alabama, AFCEA – Colorado Springs.

## Description:

Malware continues to advance in sophistication. Well-engineered malware can obfuscate itself from the user and the OS. Volatile memory is the unique structure malware cannot evade. I have engineered a new construct for memory analysis and a new open-source tool that automates memory analysis, correlation, and user-interaction to increase investigation accuracy, reduce analysis time and workload, and better detect malware presence from memory. This talk demos a new visualization construct that creates the ability to interact with memory analysis artifacts. Additionally, this talk demos new, very impactful data XREF and a system manifest analysis features. Data XREF provides an index and memory context detailing how your search data is coupled with processes, modules, and events captured in memory. The System Manifest distills the analysis data to create a new memory analysis snapshot and precise identification of malicious artifacts detectable from malware execution especially useful for exploit dev and malware analysis!

Audience: Malware Analysts/Software Reverse Engineers Exploit Developers CTF Subject Matter Experts Incident Responders Digital Forensics Examiners Offense & Defense

---

[Return to Index](#) - Add to



- ics [Calendar](#) file

---

## CPV - Sunday - 10:30-10:59 PDT

---

**Title:** XR Technology Has 99 Problems and Privacy is Several of Them (PRE-RECORDED)

**When:** Sunday, Aug 14, 10:30 - 10:59 PDT

**Where:** Flamingo - Vista Ballroom

**Speakers:**Suchi Pahi,Calli Schroeder

### **SpeakerBio:**Suchi Pahi

Suchi Pahi is a data privacy and cybersecurity attorney with a passion for tech. Her goal at conferences is to make privacy and cybersecurity law more accessible and transparent for people who are directly impacted by these legal frameworks, and to explore new developments on the tech side. She has a depth of experience in managing cybersecurity incident response and health privacy regulatory issues, as well as in building effective cybersecurity and privacy programs, partnering with product teams to create products that embed privacy, and counseling clients on privacy, cybersecurity, intellectual property, and other implications of new technologies or services.

She is currently Senior Privacy & Product Counsel at Databricks, Inc. Suchi is not speaking on behalf of Databricks, Inc., but in her own capacity.

### **SpeakerBio:**Calli Schroeder

Calli Schroeder is a privacy attorney focusing on the connection to human rights, emerging tech, and international law. Through writing, conferences, presentations, and Twitter threads, she tries to make privacy issues clear and understandable. Through work at the IAPP, FTC, law firms, and compliance companies, she has tracked international privacy developments, worked on online speech and intellectual property issues, created data maps for clients, built and run privacy programs, and drafted privacy policies, terms of use, and data protection addenda.

She is currently Global Privacy Counsel at The Electronic Privacy Information Center (EPIC).

## Description:

We've all heard, seen, and probably played in "the metaverse." The metaverse is a type of extended reality (XR), like virtual reality or augmented reality. Some of you may have wondered: Where is my information going? What kinds of things does XR tech know about me? What XR information about me is accessible to private companies and to the government? Do

privacy laws protect me in the metaverse?

Over the last two years, we've looked at various pieces of XR tech and where it intersects with the law. We have several answers for you, none of them satisfying, and each one raising even more questions.

Come join us for a wild ride to explore how extended reality plays both within and outside of existing privacy regulations, the rights you might have, and what we really need from legislators and companies to protect your privacy.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## **BTW - Friday - 16:45-16:59 PDT**

---

**Title:** YARA Rules to Rule them All

**When:** Friday, Aug 12, 16:45 - 16:59 PDT

**Where:** Virtual - BlueTeam Village - Talks

**SpeakerBio:** Saurabh Chaudhary

With over 5 years of experience protecting Banks and the financial sector against cyber threats, Saurabh Chaudhary is a renowned Security Researcher and a prominent speaker and trainer. He is a published researcher with multiple research papers on malware, ransomware, and cyber espionage and has experience and expertise in cyber threat intelligence, Malware, YARA rules, DFIR, etc.

### **Description:**

Whenever we want to proactively hunt for malware of interest for threat intelligence purposes, YARA is the swiss-army knife that makes the work of malware researchers and threat intelligence Researchers easier.

We will talk about leveraging the YARA to detect the future version of the malware. Malware developers work just like legitimate software developers, aiming to reduce the time wasted on repetitive tasks wherever possible. That means they create and reuse code across their malware. This has a pay-off for malware hunters and threat intelligence researchers, we can learn how to create search rules to detect this kind of code reuse, Traditional Yara rules are written on strings, but if we implement code leveraging YARA code reuse rules in addition to the strings rule the rule will last decades. We can leverage that for finding future malware from the same authors using their digital code fingerprints.

Malware developers work just like legitimate software developers, aiming to reduce the time wasted on repetitive tasks wherever possible. That means they create and reuse code across their malware. This has a pay-off for malware hunters and threat intelligence researchers, we can learn how to create search rules to detect this kind of code reuse, Traditional Yara rules are written on strings, but if we implement code leveraging YARA code reuse rules in addition to the strings rule the rule will last decades.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## **DC - Saturday - 15:00-15:45 PDT**

---

**Title:** You Have One New Appwntment - Hacking Proprietary iCalendar Properties

**When:** Saturday, Aug 13, 15:00 - 15:45 PDT

**Where:** Caesars Forum - Academy 401-410, 421 (Track 3)

**SpeakerBio:** Eugene Lim , Cybersecurity Specialist, Government Technology Agency of Singapore

Eugene (spaceraccoon) hacks for good! At GovTech Singapore, he protects citizen data and government systems through security research. He also develops SecOps integrations to secure code at scale. He recently reported remote code execution vulnerabilities in Microsoft Office and Apache OpenOffice and discussed defensive coding techniques he observed from hacking Synology Network Attached Storage devices at ShmooCon.

As a bug hunter, he helps secure products globally, from Amazon to Zendesk. In 2021, he was selected from a pool of 1 million registered hackers for HackerOne's H1-Elite Hall of Fame. Besides bug hunting, he builds security tools, including a malicious npm package scanner and a social engineering honeypot that were presented at Black Hat Arsenal. He writes about his research on <https://spaceraccoon.dev>.

He enjoys tinkering with new technologies. He presented "Hacking Humans with AI as a Service" at DEF CON 29 and attended IBM's Qiskit Global Quantum Machine Learning Summer School.

Twitter: [@https://twitter.com/spaceraccoonsec](https://twitter.com/spaceraccoonsec)

## Description:

First defined in 1998, the iCalendar standard remains ubiquitous in enterprise software. However, it did not account for modern security concerns and allowed vendors to create proprietary extensions that expanded the attack surface.

I demonstrate how flawed RFC implementations led to new vulnerabilities in popular applications such as Apple Calendar, Google Calendar, Microsoft Outlook, and VMware Boxer. Attackers can trigger exploits remotely with zero user interaction due to automatic parsing of event invitations. Some of these zombie properties were abandoned years ago for their obvious security problems but continue to pop up in legacy code.

Furthermore, I explain how iCalendar's integrations with the SMTP and CalDAV protocols enable multi-stage attacks. Despite attempts to secure these technologies separately, the interactions that arise from features such as emailed event reminders require a full-stack approach to calendar security. I conclude that developers should strengthen existing iCalendar standards in terms of design and implementation.

I advocate for an open-source and open-standards approach to secure iCalendar rather than proprietary fragmentation. I will release a database of proprietary iCalendar properties and a technical whitepaper.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## DC - Friday - 13:00-13:45 PDT

---

**Title:** You're <strike>Muted</strike>Rooted

**When:** Friday, Aug 12, 13:00 - 13:45 PDT

**Where:** Caesars Forum - Alliance 301-309, 321 (Track 4)

**SpeakerBio:** Patrick Wardle , Founder, Objective-See Foundation

Patrick Wardle is the creator of the non-profit Objective-See Foundation, author of the “The Art of Mac Malware” book series, and founder of the “Objective by the Sea” macOS Security conference.

Having worked at NASA and the NSA, as well as presenting at countless security conferences, he is intimately familiar with aliens, spies, and talking nerdy.

Patrick is passionate about all things related to macOS security and thus spends his days finding Apple 0days, analyzing macOS malware, and writing free open-source security tools to protect Mac users.

Twitter: [@https://twitter.com/patrickwardle](https://twitter.com/patrickwardle)

## Description:

With a recent market cap of over \$100 billion and the genericization of its name, the popularity of Zoom is undeniable. But what about its security? This imperative question is often quite personal, as who amongst us isn't jumping on weekly (daily?) Zoom calls?

In this talk, we'll explore Zoom's macOS application to uncover several critical security flaws. Flaws, that provided a local unprivileged attacker a direct and reliable path to root.

The first flaw, presents itself subtly in a core cryptographic validation routine, while the second is due to a nuanced trust issue between Zoom's client and its privileged helper component.

After detailing both root cause analysis and full exploitation of these flaws, we'll end the talk by showing how such issues could be avoided ...both by Zoom, but also in other macOS applications.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## HRV - Friday - 11:30-12:30 PDT

---

**Title:** Your Amateur Radio License and You

**When:** Friday, Aug 12, 11:30 - 12:30 PDT

**Where:** Flamingo - Virginia City II

**SpeakerBio:** Justin/InkRF

Justin (AKA "InkRF") is studying electrical engineering and is an amateur extra class ham radio operator. Since entering the hobby in 2020, he has been involved with many amateur radio organizations around the country and world, including serving on the board of the Ham Radio Village and on the HRV conference committee. While Justin enjoys operating a pileup, his main mission in the hobby is getting others to learn more about, and join the endless world that is amateur radio.

Twitter: [@https://twitter.com/InkRF](https://twitter.com/InkRF)

<https://inkrf.net/>

## Description:

Once you acquire an amateur radio license (otherwise known as ham radio), many are left to wonder what to do next. This presentation will cover some of the basic/fundamental topics to know once you get your amateur radio license and how to use it. Hopefully after you leave this presentation you may overcome that "mic fright" many hams get once they get their license, and their hands on a radio.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## PT - Tuesday - 09:00-16:59 PDT

---

**Title:** Zero 2 Emulated Criminal: Intro to Windows Malware Dev

**When:** Tuesday, Aug 16, 09:00 - 16:59 PDT

**Where:** Caesars Forum

**SpeakerBio:** Dahvid Schloss

Dahvid is the Offensive Security Lead at Echelon Risk + Cyber. As an experienced professional with over 12 years of cyber-attack and defense experience, Dahvid has previously worked as a Red Team Operator with a Big 4 consulting firm

leading and conducting Adversarial Emulation exercises. He also served in the military, leading, conducting, and advising on special operations offensive cyber operations. He has a wide background in cyber security including logical, social, and physical exploitation as well as leading malware development enabling c2 execution while evading endpoint detection solutions.

## Description:

Latest details, requirements, description, cost:

<https://defcontrainings.myshopify.com/products/dahvid-schloss-zero-2-emulated-criminal-intro-to-windows-malware-dev-1>

Training description:

Step up your emulated criminal game with a practical, hands-on introduction to malware development. Join a prior US Special Operations Cyber Operator to learn the building blocks and techniques used in real-world malware variants. You don't need fancy, expensive tools to get a C2 implant executed while evading antivirus. You need basic knowledge, ingenuity, and elbow grease. In this course, we don't cut corners. You will learn by doing, not by copying and pasting with modules and labs that will give you the ability to deviate and improvise on your very first malware variants in C++, even if you have no prior C++ experience. Where this course differs from others is its reduced need for prior knowledge, and enhanced emphasis on hands-on learning. By the end of the course, you will understand and be able to implement:

- Techniques to use the native Win32 API for adversarial tactics, enhancing stealth and offensive efficiency
- Maintaining data/shellcode integrity while using multiple ciphers for obfuscation and encryption
- Modular antivirus evasion techniques that will remain useful through your pen testing career

---

[Return to Index](#) - Add to



- ics [Calendar](#) file

---

## PT - Monday - 09:00-16:59 PDT

---

**Title:** Zero 2 Emulated Criminal: Intro to Windows Malware Dev

**When:** Monday, Aug 15, 09:00 - 16:59 PDT

**Where:** Caesars Forum

### SpeakerBio:

Dahvid Schloss

Dahvid is the Offensive Security Lead at Echelon Risk + Cyber. As an experienced professional with over 12 years of cyber-attack and defense experience, Dahvid has previously worked as a Red Team Operator with a Big 4 consulting firm leading and conducting Adversarial Emulation exercises. He also served in the military, leading, conducting, and advising on special operations offensive cyber operations. He has a wide background in cyber security including logical, social, and physical exploitation as well as leading malware development enabling c2 execution while evading endpoint detection solutions.

## Description:

Latest details, requirements, description, cost:

<https://defcontrainings.myshopify.com/products/dahvid-schloss-zero-2-emulated-criminal-intro-to-windows-malware-dev-1>

Training description:

Step up your emulated criminal game with a practical, hands-on introduction to malware development. Join a prior US Special Operations Cyber Operator to learn the building blocks and techniques used in real-world malware variants. You don't need fancy, expensive tools to get a C2 implant executed while evading antivirus. You need basic knowledge, ingenuity, and elbow grease. In this course, we don't cut corners. You will learn by doing, not by copying and pasting with modules and labs that will give you the ability to deviate and improvise on your very first malware variants in C++, even if you have no prior C++ experience. Where this course differs from others is its reduced need for prior knowledge, and enhanced emphasis on hands-on learning. By the end of the course, you will understand and be able to implement:

- Techniques to use the native Win32 API for adversarial tactics, enhancing stealth and offensive efficiency
- Maintaining data/shellcode integrity while using multiple ciphers for obfuscation and encryption
- Modular antivirus evasion techniques that will remain useful through your pen testing career

Win32 API for adversarial tactics, enhancing stealth and offensive efficiency - Maintaining data/shellcode integrity while using multiple ciphers for obfuscation and encryption - Modular antivirus evasion techniques that will remain useful through your pen testing career

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## DL - Friday - 10:00-11:55 PDT

---

**Title:** Zuthaka: A Command & Controls (C2s) integration framework

**When:** Friday, Aug 12, 10:00 - 11:55 PDT

**Where:** Caesars Forum - Society Boardroom

**Speakers:**Lucas Bonastre,Alberto Herrera

### **SpeakerBio:**Lucas Bonastre

Lucas started his career studying Mathematics at the University of Buenos Aires, however when his uncle gave him a C++ book, he realized his true passion for programming and his outstanding ability for problem-solving. He worked across cybersecurity and technology firms and is a vetted developer in many languages such as C/C++, Python, Java, and PHP. Now he is a full time developer and security researcher at Pucara Information Security. In his spare time, he is an expert chess player, and he is studying Computer Vision to analyze foosball strategies.

### **SpeakerBio:**Alberto Herrera

Alberto began his journey in cybersecurity in a consulting firm, where he worked with one of the biggest telecommunication companies of the region. He continued as an advisor on the National Cyber-Defence Initiative for the Argentina Armed Forces where he worked on many high-level government programs which required elevated security clearance. He also worked for Immunity, a prominent offensive security firm that serves the financial sector, and large enterprises, where he performed cybersecurity assessments for Forbes 100 companies. In his spare time, he is a retro gaming evangelist, where he applies his hardware-hacking and low-level programming skills on different architectures.

### **Description:**

The current C2s ecosystem has rapidly grown in order to adapt to modern red team operations and diverse needs (further information on C2 selection can be found [here](#)). This comes with a lot of overhead work for Offensive Security professionals everywhere. Creating a C2 is already a demanding task, and most C2s available lack an intuitive and easy to use web interface. Most Red Teams must independently administer and understand each C2 in their infrastructure. Zuthaka presents a simplified API for fast and clear integration of C2s and provides a centralized management for multiple C2 instances through a unified interface for Red Team operations. A collaborative free open-source Command & Control development framework that allows developers to concentrate on the core function and goal of their C2. Zuthaka is more than just a collection of C2s, it is also a solid foundation that can be built upon and easily customized to meet the needs of the exercise that needs to be accomplished. This integration framework for C2 allows developers to concentrate on a unique target environment and not have to reinvent the wheel. After we first presented Zuthakas' MVP at Black hat USA 2021 and DEFCON demo labs, we are now presenting the first release with updated post-exploitation modules to support text based modules, as well as file based ones. With a lab populated of commonly used C2s and its out-of-the-box integrations.

Audience: Red team operators, wishing a centralized place to handle all C2s instances. C2 developers, wishing to save the effort of writing the Frontend. Hackers, wishing a strong infrastructure to run C2s.

---

[Return to Index](#) - Add to [Google Calendar](#) - ics [Calendar](#) file

---

## DEF CON Transparency Report Update

Posted 7.28.22



In preparation for DEF CON 30, we've updated the [transparency report](#) on the DEF CON website. While you're there, take a moment to re-familiarize yourself with the [code of conduct](#). We don't have a ton of rules, but we take the ones we have very seriously.

## DEF CON 30 Speaking Schedule is Live!

Posted 7.15.22

A screenshot of the DEF CON website showing the speaking schedule for Friday, August 12th, 2022. The page has a dark header with "SH3DULE" and the DEF CON logo. Below the header, there are tabs for "HOME", "OPEN CALLS", "FAQ", and "VENUE". Under "OPEN CALLS", it says "DEF CON 30 will be August 11-14, 2022 at Caesars Palace, Flamingo, Linq, and Aria in Las Vegas, NV". On the left, there are sections for "Booking Up" and "Calling Up". The main content shows a grid of sessions: Track 1, Track 2, Track 3, and Track 4. Session details include "Panel - DEF CON Policy Draft + What are we and what are we not allowed to do at DEF CON when NOT in the city", "Old Policies, New Social Skills: Understanding CSD and Local Conference Policies", and "Computer Attacks on the Russian Ukraine and North Korea". Each session has a "Cheat Sheet" link.

'Tis the season, hackerfolk. DEF CON is almost here and all four tracks of the main speaker schedule are live on the website! Visit the [Schedule page](#) to start your planning. Our valiant CFP Review Board has put together a strong list of presentations over a wide array of subjects. We're sure you'll find plenty of interest.

Feel free to tweet at us about the talks you want to see, and feel equally to free to get hyped. Less than a month now, people.

## Floorplan Maps are Live, Room Block discount Ends Soon!

Posted 7.7.22



The [floorplan maps for DEF CON 30](#) have been added to the Venue page of the DC30 website. Take a peek and plot your course, it's just a few short weeks now.

The DEF CON 30 room rate discount closes July 15 - so book soon to take advantage of the price break! Our room block in Caesars is full, but many others still have price breaks available.

[Book a Room for DEF CON 30 Here !](#)

## COVID Clarification for DEF CON 30

Posted 6.22.22



Just so there's no confusion, DEF CON 30 will require masks, same as last year. We thank everyone for keeping each other safe last year, and we can't wait to get the gang together responsibly just a few short weeks from now.

Original [DEF CON 30 Covid Policy](#) post from May.

## First Batch of DEF CON 30 speakers is Live!

Posted 6.9.22



Friendly DEF CON 30 announcement - [the first bunch of speakers are selected](#) and available for your perusal on the DEF CON forums. Congrats to everyone already selected. Keep your eyes on this space for more selections!

## DEF CON Training Site is Live!

Posted 5.31.22



DEF CON Trainings registration is LIVE! Right after DEF CON 30, we're excited to offer these intensive 2 day classes with a certificate of completion. First come, first served so don't procrastinate. Class descriptions and reg information are at [defcontrainings.myshopify.com](https://defcontrainings.myshopify.com).

## Weekend Updates! CTF Quals news, and New SE Community Q&A Today!

Posted 5.27.22

 **Nautilus Institute**  
@Nautilus\_CTF

#defcon quals chat on the Defcon discord is open. Come visit us in #ctf-discussion-text to ask all the important questions, like "when is web?" and "this challenge is too hard unlock another one"

### CTF News

CTF Quals are almost here (May 28 at 0000 UTC) and the CTF Chat on the DEF CON discord is already open!

From [@NautilusCTF](#) :

#defcon quals chat on the Defcon discord is open. Come visit us in [#ctf-discussion-text](#) to ask all the important questions, like "when is web?" and "this challenge is too hard unlock another one"

Time is short to get to the [Nautilus Institute Website](#) and register your team for CTF quals!



SOCIAL ENGINEERING  
COMMUNITY

JOIN US! This Friday to discuss the new  
DEF CON Social Engineering Community.



JC  
Co-Founder



Snow  
Co-Founder

<https://www.se.community>

### SE Community Q&A Today!

Join Social Engineering Community Village cofounders [@JC\\_SoCal](#) and [@sn0ww](#) to talk all about what kind of events the Social Engineering Community has in store for DEF CON 30. They'll be live on Twitch answering your questions at 5pm EDT Friday the 27th at [twitch.tv/se\\_community](https://twitch.tv/se_community). See you there!

## The Black and White Ball is Back!

Posted 5.24.22

D3FC0N

**Black and White Ball  
ANNOUNCEMENT!**

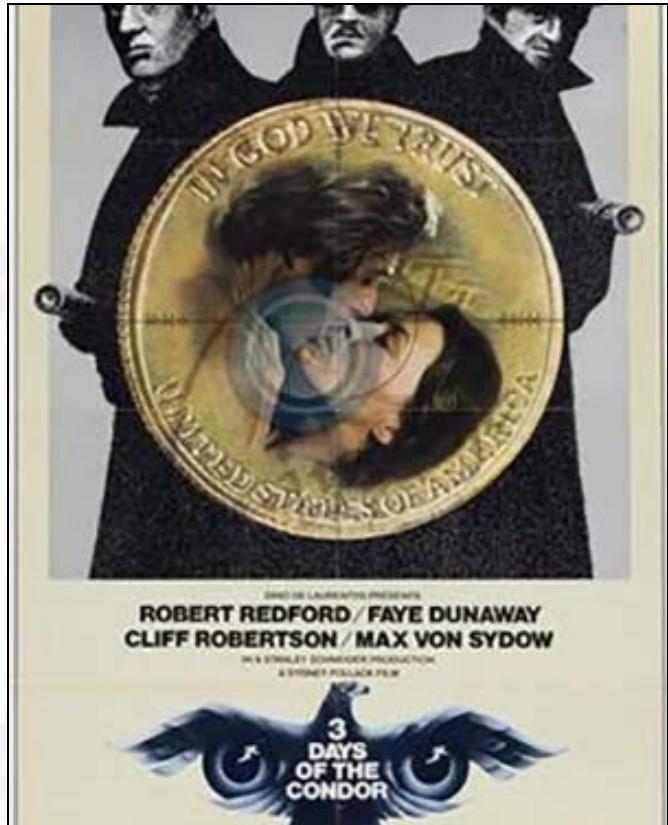
Come dressed to impress,  
and if you pass the test  
free drinks til they're gone  
**THEN we let in the rest.**

so fix up, look sharp  
more details soon!

A little announcement about DEF CON 30's Black and White Ball: the best-dressed entrants will get some to enter early and enjoy a few free drinks before we let everyone else in. So look sharp - more details to come.

## DEF CON Movie Night: 3 Days of the Condor

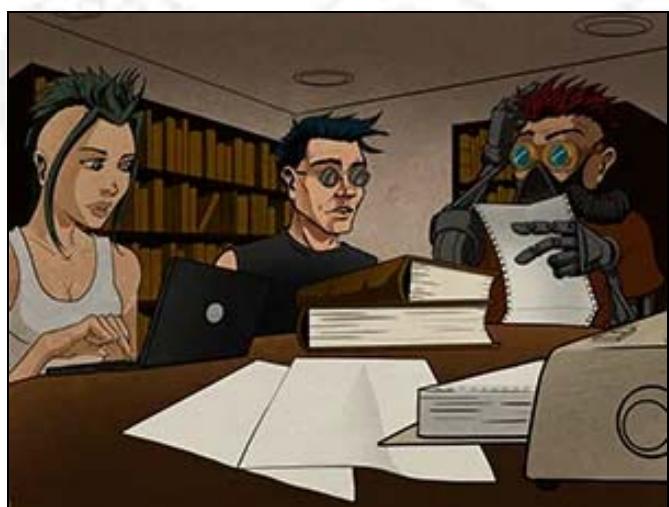
Posted 5.21.22



Join us Saturday the 21st at 8pm PDT for Sydney Pollack's 1975 spy thriller 'Three Days of the Condor'. Robert Redford plays a CIA researcher on the run and Ma Bell plays herself. We'll be hiding out in the DEF CON Discord ([discord.gg/defcon](https://discord.gg/defcon)) under the code name movie-night-text.

## Check out Policy @ DEF CON!

Posted 5.19.22



Policy matters. The world has never been so connected, and mighty forces contend for the right to shape our digital lives. DEF CON believes the hacker community needs a voice in that process. To help people learn, connect and get involved with the leading edge of tech policy, we offer '[Policy @ DEF CON](#)'. We'll have presentations, panels, and off-the-record evening lounges. Get yourself up to speed on the issues, connect with some of the players and maybe even get involved. The future is what we make it!

# The DEF CON 30 Website is live!

Posted 5.13.22



Good news, everyone! The [DEF CON 30 official website is officially LIVE](#) and DEF CON season is officially IN EFFECT. Bookmark it for a handy place to check out all of the DC30 infoz as they roll in. Check the calendar, jump into the forums, book a room - it's all in one place.

Now that we've reached cruising altitude, you are free to shimmy excitedly around the cabin.

Let's GoOOoo!

## COVID Updates for DEF CON 30

Posted 5.3.22



DEF CON 30 is getting closer, and that means we're starting to get questions about Covid-19 protocols for the in-person event. Here's the current state of play.

Some things have changed since DC29. The US has largely stopped checking vaccine status for entry to indoor events, owing

at least partly to the knowledge that the vaccines serve more to prevent severe disease than to curtail transmission. COVID-19 testing is now mostly done privately with widely available at-home kits.

But most things haven't changed. There are still new variants on the move. There are still spikes in transmission and hospitalization. Masks are still the most effective way to protect people in indoor events.

Barring a major change in the situation, we will not check proof of vaccination, but we will keep last year's mask requirement in place for DEF CON 30. Protecting the community is our first priority, and we want to make sure that everyone is as safe as we can make them. Everyone includes the healthy, the vulnerable and those who have immune compromised loved ones they need to protect.

Thank you for all you did to protect each other last year, and with your help we'll do it again this year.

## **Training Coming to DEF CON 30, Call for Training is Open!**

Posted 4.14.22



The wait is over - we're ready to announce the Call for Trainers!

This year we're adding DEF CON Training – intensive, two-day courses of study aimed at building specific skills. In some cases, these courses will even carry a certification. The Trainings will be held August 15-16, the Monday and Tuesday after DEF CON.

We're looking for unique, technical, and practical presentations from trainers with deep knowledge of their subject. If that's you, we're offering:

- 50/50 split of the gross income.
- Optional test where students demonstrate their skill for a certificate.

All the info you need to apply is on the [Call for Training](#) page. Get your applications in early – we look forward to seeing what you've got to share.

## **New Payment Option for DEF CON 30!**

Posted 3.25.22



DEF CON is a cash-at-the-door kind of conference. Paying in cash helps protect your privacy, and search warrants can't vacuum up PII we don't collect. You will always be able to lay down US dollars in the reg line and collect your badge.

Still, the experience of DC29 taught us a few things. Some of our attendees work DEF CON into their business travel schedule, and the option to pre-reg with a credit card over the web made things much easier for them. Some of our attendees need to manage a group purchase, or want a more detailed receipt.

For everyone who fits into those categories, we're happy to announce that we're keeping the option of online registration. Starting Monday, March 28th, you'll be able to use [shop.defcon.org](https://shop.defcon.org) to buy your ticket and get your receipt. We hope the online option makes the process more streamlined for those who need it. We thank people for their patience and feedback as we navigate the changing landscape.

The price for DEF CON 30 is \$360, with a processing fee of \$9.66 added to online orders.

*Fine print: Currently we cannot provide beachballs and pizza to the online purchasing experience. For that, you're gonna need LineCon.*

## DEF CON Movie Night: Dark Star!

Posted 3.16.22



DEF CON Movie Night this Saturday will feature some more 70s sci-fi with John Carpenter's 'Dark Star' from '74. Join us 3-19 at 8pm PDT in the #defcon discord ([discord.gg/defcon](https://discord.gg/defcon)). We'll be in the movie-night-text channel.

## Villages for DEF CON 30!

Posted 3.15.22



The list of [DEF CON 30 villages on the Forums](#) has been updated! Stop by to check out the full complement of village goodness we're offering this year. Comment, like, subscribe, volunteer to help out - but mostly get amped. #defcon30approaches.

## Coming soon: Call for Training!

Posted 3.11.22



We're excited to announce something new on the menu for DC 30 - DEF CON Training! We're launching a lineup of intense two-day trainings taking place August 15-16 in the same venue, and we're looking for trainers!

**WHAT:** DEF CON We're seeking Trainers for two-day training sessions right after DEF CON 30.

**WHEN:** August 15-16, the Monday and Tuesday after DEF CON 30.

**WHERE:** Same location, the Caesars Forum.

**WHY:** For DEF CON attendees who love our free Workshop series but wish they could get an even deeper, more focused dive and maybe even a certificate. Like everything we do at DEF CON, we hope it will help to build and strengthen the hacker community and spread the kind of knowledge that makes the world more open and secure.

DEF CON Training will offer two-day paid training courses in the \$1-\$3k price range. We're looking for unique, technical, and practical presentations from trainers with deep knowledge of their subject. If that's you, we're offering:

- 50/50 split of the gross income.
- Optional test where students demonstrate their skill for a certificate.

Interested? We will launch the Trainer submission form later this month! If you have questions, drop us a line at [info@defcon.org](mailto:info@defcon.org).

The Dark Tangent

## More DEF CON 30 Calls Opening!

Posted 2.15.22



Good news, everyone! We have more calls open for DEF CON 30!

**Call for Parties and Meetups** : your dreams of throwing an epic party at DEF CON 30 are within your reach! If you have a solid concept to wrap some next level festivities around, get at us. The best ideas will get space and support. Details here: [Call for Parties](#)

**Call for Music** : we're gonna need some tunes. Lots of tunes. This call is for established acts and bedroom Beethovens alike. We're looking for live performers, so if you've got the stuff that puts the dip in our hip and the glide in our stride, get to the [Call for Music](#) and let us know.

**Call for Vendors** : we're always looking for new hacker gear and accessories to share with the community. Get your cool swag in front of a pretty savvy and curious audience by applying here at the [Vendor Application](#)

## New Calls Open for DEF CON 30!

Posted 2.1.22



You know how you can tell it's DEF CON season? The Calls. When you hear the distinctive warble of the DEF CON Content calls, you know what's up. It's like the first robin of spring, if robins were cooler and more hacker-focused.

Today we're opening three more DEF CON 30 Calls:

#### **Call for Papers**

The big one. If you want to speak at DEF CON 30, it's time to get your submission together. As always, we're looking for fresh, technical content and the sooner you get it in, the better your chances. We can offer suggestions to help you get over the finish line, time permitting. Fortune favors the bold, so don't delay.

#### **Call for Workshops**

The very popular workshop series is back for DEF CON 30. Some topics need a more time and involvement than a main-stage talk can offer. The workshops are an amazing way to share your in-depth, hands-on content with the DEF CON community.

#### **Demo Labs**

Get your open source project in front of the knowledgeable, curious humans of DEF CON. Get valuable feedback, find accomplices and raise your project's profile. We provide the floor space and the audience, you provide the timely submission.

The DEF CON machine is revving up, and DC30 will be here before you know it. Don't miss your chance to get involved. The community is waiting to see what you've got to share.

## **A Warm Welcome to the Next CTF Organizer Team: Nautilus Institute!**

Posted 1.28.22

# WELCOME Nautilus Institute

@

Big DEF CON 30 CTF update! Following several years of exemplary service by the Order of the Overflow, our world-famous Capture the Flag contest is under new management. The care and feeding of this year's CTF is in the worthy and capable hands of the Nautilus Institute!

From Nautilus Institute:

**Ahoy DEF CON and CTF communities!**

We are the Nautilus Institute. We have been chosen, from a very respectable pool of applicants, to steer the DEF CON CTF ship starting in 2022. We are thankful for this honor, and hope to navigate straight and true no matter what waters lie ahead.

We're a bit light on details, while we prepare for this year's DEF CON CTF Qualifiers May 28-29, but we hope to flag you down with more information soon! Please follow us on twitter at [https://twitter.com/Nautilus\\_CTF](https://twitter.com/Nautilus_CTF) and keep a look out on our website at <https://nautilus.institute>.

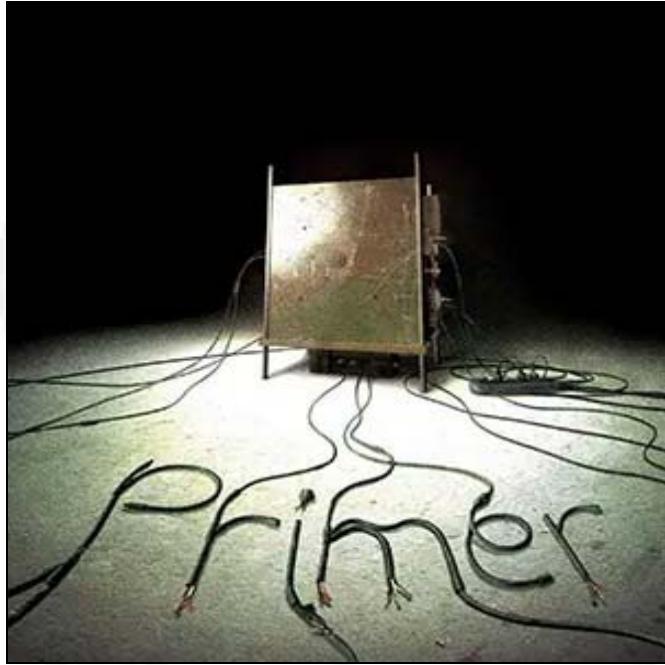
Sea you soon,

@•§

For the boldest and best prepared, glory awaits. Godspeed.

## DEF CON Movie Night: Primer!

Posted 1.27.22



DEF CON movie night rolls on with 'Primer'. Joins us on the [DC discord](#) Saturday 8pm PST for what has to be the most brainmelting time travel movie that could possibly be shot for \$7000. Bring a cork board and a few different colors of yarn. We'll be waiting for you in the movie-night-text channel.

## DEF CON Movie Night: Tank Girl!

Posted 1.19.22



This week's DEF CON movie night will feature the very weird 'Tank Girl' from 1995. Join us Saturday, 8pm PST in the movie-night-text channel of the [DEF CON discord](#) for a glimpse at what the apocalypse looked like from the more innocent viewpoint of the mid 90s. Bring your own water.

## DEF CON New Year's Eve!

Posted 12.23.21



DEF CON is doing a small [New Year's Eve event](#) on the DEF CON discord. There will be several hangouts and contests to participate in. We'll have music, a Kubernetes CTF, A Ham radio CTF, some Hacker Karaoke, movie watchalongs and more. We'll have the full rundown on defcon.org and we'll update in the NYE Forum threads. Join us in welcoming 2022 - can't wait to see you!

## DEF CON 29 Transparency Report

Posted 12.6.21



The full DEF CON [Transparency Report for DEF CON 29](#) is now available. Our deepest thanks to everyone who reported issues to us and also to the people on staff who tracked down and handled those issues. It's a community effort, and it's good to see the progress we're making.

# DEF CON Ornament Now Available!

Posted 11.23.21



The holiday season is upon us - time to spruce up your place with some festive hacker accents. This is the only [official DEF CON ornament](#). Accept no substitutes. Suitable for all celebrations and a welcome addition to any decor.

## Enter the DEF CON 30 Artwork Contest!

Posted 11.17.21



Now that the DEF CON 30 Theme is out there in the world, it's time to go pencils up on the DEF CON Art Contest!

This year's theme is 'Hacker Homecoming' , and you can read all about it on the DEF CON Forums. It's a theme meant to celebrate our community's much awaited reunion next August. It's also meant to reference the 30th Anniversary we're celebrating, which is a pretty big deal for a hacker conference.

So if you've got some art skills, you've got a luxurious 7+ months to get your take on the theme in to us. There's so much time between now and the June 1 deadline that you could probably learn a brand new art style in which to make your submission. You can drop as many submissions to [pictures@defcon.org](mailto:pictures@defcon.org) as you want, so enter early and often.

### ### Theme:

We are looking for artwork that reflects a spirit of community and reunion. We're looking for art that combines the 90's

hacker aesthetic of DEF CON's history and our tribe's 21st century future. We're looking for your vision and vibes.

We hope you'll take in the information in [the style guide](#), but we hope that you'll use that as a launching pad and not a set of limits. We want to see where you can take these ideas.

### ### Guidelines:

300 DPI. Convert type to outlines where applicable. Trust your instincts - we're looking for genuine energy, not technical perfection. We want to share and amplify the artists in our community. If that's you, get your ideas down. If that's not you yet, could it be? You've got a few months to find out.

Entries will be placed on the DEF CON Forums for voting, and there will be prizes. There will also be gratitude, and opportunities to inspire others with your special way of seeing the world. We can't wait to see what you'll make!

## DEF CON 30 Theme: Hacker Homecoming

Posted 11.12.21



This has been a crazy couple of years.

A global pandemic turned DEF CON 28 into DEF CON Safe Mode. Some easing of the restrictions and some strict attendance rules gave us a hybrid con for DC29. An improvement, to be sure, but something short of a full DEF CON experience.

We want DEF CON 30 to have the energy of a reunion. We'll be back together in a brand spanking new venue. We'll be thirty years old - an amazing milestone for a hacker conference under any circumstances. In honor of all that, we're calling DEF CON 30 'Hacker Homecoming'.

The first reason is that it's literally a return home. After two years of separation, we're looking forward to having more of our family under one roof, under the Vegas late summer sun.

There's also a North American tradition called 'Homecoming'. Secondary schools and colleges invite luminary alums back for a big celebration of the school's history and a toast to its future. We intend to do just that for DC30. We'll have some surprise guests from DEF CON's illustrious past on hand to talk about the amazing places their life has taken them since joining the DC Community. We'll also be laying out some of the map forward from our 30th Anniversary.

So please join us in the Caesar's Forums if you can, and on the Discord if you can't. Maybe even pack a fancy outfit for the homecoming dance. It's high time for a reunion.

## Design Inspiration

This year's theme is about celebrating the past and getting geeked about the future, so we're looking for smooth integration of old school hacker style with future vibes.

We took the color palette inspiration from arguably the most iconic DEF CON image of all time: the rooftop photo from DEF CON 1.

The photo is amazing for any number of reasons, but the most important is that even though it screams early 90s hacker culture, it also shows some of the essence of what DEF CON is even in the 2020s. It's still a gathering of extraordinary digital misfits going Voltron in the Vegas night.

The fonts were also selected to be like a homecoming celebration, with some reverence for the past, some excitement about the future. The past is represented by the very 90s CityPop and Geom and the future by the futuristic minimalism of Open Sans.

## Homework

As always, we'll be sharing movies, books, music and other random media to get you in the right frame of mind for maximum DEF CON. This year we're even giving you an extra few months to get through the syllabus. Watch the DEF CON site for additions to all the lists. Pencils UP!

### Movies:

Sneakers  
The Imitation Game  
Zero Days

### Books:

The Shockwave Rider  
The Cuckoo's Egg  
Kingpin: How One Hacker Took Over the Billion-Dollar Cybercrime Underground  
The Cult of the Dead Cow

## The DEF CON 30 Call for Contests and Events is OPEN!

Posted 11.1.21



DEF CON 30 is going to be a big deal, and we're full speed ahead on planning. If you've got a stellar idea for a contest, this is your moment. Take advantage of the early opening to turn your idea into a real DEF CON Experience. The extra lead time helps us work with you to get the best ideas across the finish line, but only if you take advantage and get your submissions in.

You can read the rules and requirements on the [Call for Contests Page](#). You can check the [DC29 Contest forum](#) for an idea of what we've accepted in the past.

Let's see what you've got percolating out there, DEF CON fam. Let's take DC30 up a notch.

## Happy Halloween from DEF CON

Posted 10.31.21

WISHING YOU  
AN EXTRA SPOOKY  
HALLOWEEN



## DEF CON 30: Open and Upcoming Calls

Posted 10.26.21



The DEF CON 30 Call for Villages is already open! To see if your fave is already accepted, check out the [Villages forum for DEF CON 30](#) ! Don't see what you want on the current list? Maybe that's your cue to [submit a proposal](#) !

For the truly ambitious, there is still a [call open for the coveted title of CTF organizers](#) ! Only a little over two weeks left to put in your proposal to be the future of DEF CON Capture the Flag!

On the horizon very soon will be the Call for Contests! Polish those proposals for new DEF CON contests now and be ready for the call!

We only turn 30 once. Let's do it big!

## **DEF CON 30 Call for Villages has Opened!**

Posted 10.1.21



DEF CON 30 may seem a long way off, but it's never too soon to start planning. Especially for something as close to the heart of the DEF CON experience as Villages.

As always, we're looking for new villages that will create welcoming, hands-on spaces for congoers to sharpen their skills, learn something new and maybe even find their newest obsession.

Space (both physical and metaphorical) is limited. Early submissions have increased chances of success. If the concept is strong but needs work, we can help but only if we have enough time.

You'll want to familiarize yourself with the requirements and submission guidelines at <https://defcon.org/html/defcon-30/dc-30-cfv.html> first. If you can meet the preconditions, and you have a stellar idea to propose, that's the universe telling you it's go time. Rise to meet your moment.

We can't wait to see what's on your mind.

## **CTF Call for Organizers is Officially Open!**

Posted 9.28.21



The mighty and venerable Order of the Overflow is retiring from organizing the DEF CON CTF, and the torch must be passed. This means a rare opportunity for you, CTF enthusiasts.

Are you ready to create the next generation of elite CTF tournaments? Do you have the skill and creativity to elevate the game for the world's best players? The drive to see your ideas through to completion? If this is you, it's time for us to talk.

The lowdown is at <https://defcon.org/html/links/dc-ctf-cfo.html>. Get familiar, submit the CTF you want to see in the world. For the chosen, glory awaits.

## Live Music from DEF CON 29 is Posted!

Posted 9.16.21



The [live music from DEF CON 29](#) is now available on the DEF CON Media Server! Whether you missed the party in Vegas or you just need a gang of .flac bops for your earbuds, media.defcon.org has you covered.

Get some, shake your groove things and pass it on.

## Car Hacking and Blue Team Village Talks from DEF CON 29!

Posted 9.12.21



More DEF CON 29 Village videos on the DEFCONConference YouTube channel - this time it's the [Blue Team Village](#) and [The Car Hacking Village](#)! Please enjoy and share with everyone you think could gain from the information.

## More Village Talks from DEF CON 29!

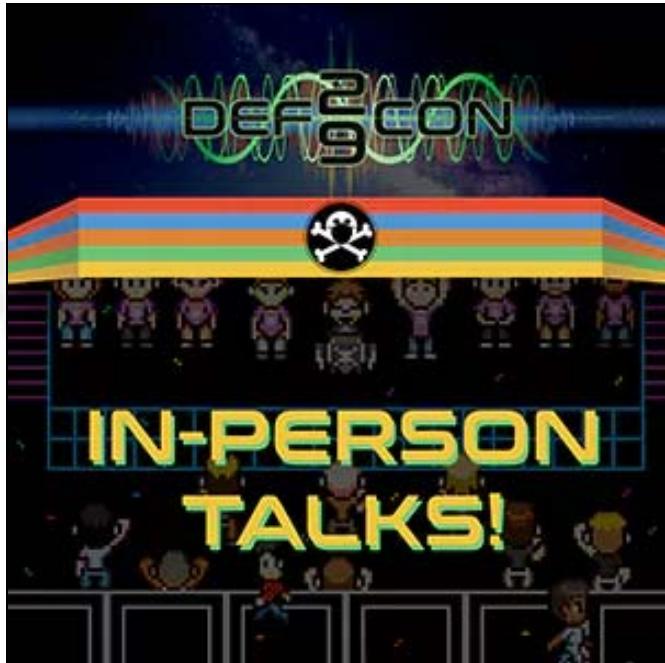
Posted 9.5.21



The Village talks deluge continues, with talks from [IoT Village](#), [Blacks in CyberSecurity Village](#), and [Aerospace Village](#) all ready to stream to your heart's content on YouTube! As always, enjoy and pass it on.

## In-person Talks from DEF CON 29 Now Live on YouTube!

Posted 8.31.21



The [in-person talks from DEF CON 29](#) are now live on the DEF CON YouTube Channel! Time to catch up on some mighty fine panels and unique content you had to be in Vegas to see..UNTIL NOW!

## **Press Page Updated for DEF CON 29!**

Posted 8.23.21



DEF CON 29 was about two weeks ago - thanks again to everyone who helped make a success of it both in person and online. We've updated the [press page](#) to include a bunch of later-breaking stories. Watch this space for a list of write ups!

## **Adversary Village Talks are Live!**

Posted 8.17.21





More DEF CON 29 goodies for your enjoyment - the [talks from Adversary Village](#) are live on our YouTube channel ! Binge away - more Village goodness to come!

## DEF CON 29 Contest results So Far!

Posted 8.13.21



Congratulations to everyone who participated in any of the DEF CON 29 contests. Getting in the ring is 90 percent of the magic, and we hope that everyone had fun, learned something and met cool new people.

The [contest results](#) we have so far have been posted, and we'll be updating the page as we get more in!

# Thanks for a Great DEF CON 29!

Posted 8.10.21



The past few years have been crazy, but you can't stop the signal, even with global cataclysm. We are so happy to be reunited with so many of our friends, both here in Las Vegas and in the virtual con space. It's good to be together.

Thank you for your support through everything. Your unending enthusiasm sustains our work and the DEF CON community never disappoints. Thanks for following the stricter rules the pandemic made necessary. Thanks for being kind and patient with each other and with us as we navigate the swiftly changing landscape.

Next year is a big anniversary for DEF CON, and we're already at work planning how to make the big 3-0 memorable. Here's to next year reuniting even more of us.

In the meantime, keep in touch with us on the DEF CON Discord server. Join a local DC Group, or start one. Stay safe and healthy. DEF CON hearts you.

## Interviews from DEF CON 29!

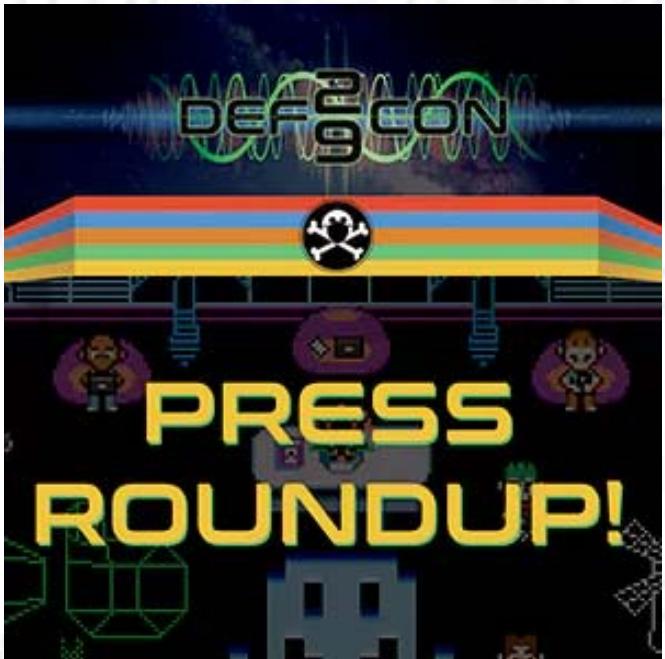
Posted 8.9.21



We'd like to shout out newly minted Photogoon Alex Chaveriat aka 'Silk' who spent his DEF CON 29 racing around the con floor finding cool projects to interview people about. If you follow the DC social media feeds you've probably seen some of his work this year. Thanks to everyone who gave him some time, and thanks to Alex for putting out so much quality stuff so quickly. [Alex Chaveriat on YouTube](#)

## DEF CON 29 Press roundup!

Posted 8.8.21



We're on the last day of DEF CON 29, both in the virtual and physical worlds. There's so much going on it's easy to miss a few things. Here's a brief listing of some of the press coverage of our events this year.

[AND!XOR's DEF CON 29 Electronic Badge Is An Assembly Puzzle](#)  
Hackaday

[Hands On: DEF CON 29 Badge Embraces The New Normal](#)

Hackaday

[Black Hat USA 2021 and DEF CON 29: What to expect from the security events](#)

Tech Republic

[Privacy Without Monopoly: DEFCON 29](#)

EFF

[We Have Questions for DEF CON's Puzzling Keynote Speaker, DHS Secretary Mayorkas](#)

EFF

[Hands-On: Whiskey Pirates DC29 Hardware Badge Blings With RISC-V](#)

Hackaday

[#DEFCON: Hacking RFID Attendance Systems with a Time Turner](#)

infosecurity

[#DEFCON: Why Social Media Security is Election Security](#)

infosecurity

[#DEFCON: A Bad eBook Can Take Over Your Kindle \(or Worse\)](#)

infosecurity

[#DEFCON: Ransomware Moves from Nuisance to Scourge](#)

infosecurity

[Black Hat USA 2021 & DefCon 29: Hybride IT-Security-Konferenzen starten in Kürze](#)

Heise.de

[The Cybersecurity 202: The year's biggest cybersecurity conferences are back, but limited](#)

The Washington Post

## **DEF CON 29 Badge Update (The Firmware Kind)!**

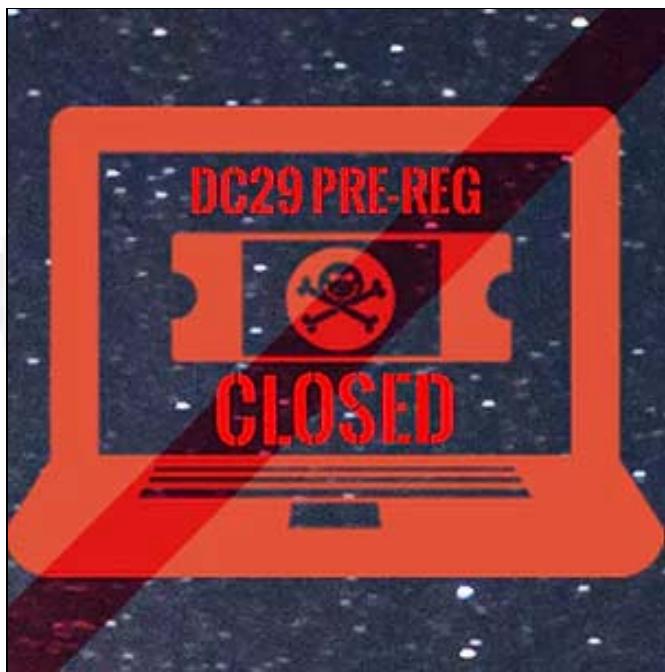
Posted 8.5.21



In case you didn't know, you can head over to [defcon.org/signal](https://defcon.org/signal) for a link to updated badge firmware and instructions! We hope you enjoy DEF CON 29, In-person, or from wherever you may be!

## DEF CON 29 In-person Pre-Registration is Closed!

Posted 8.4.21



The DEF CON 29 pre-reg at [shop.defcon.org](https://shop.defcon.org) is now closed. You can still get a badge with cash payment onsite while they last, and you can purchase the Human+ Discord role directly on our Discord ([discord.gg/defcon](https://discord.gg/defcon)) or at [plus.defcon.org](https://plus.defcon.org). Thanks to everyone for supporting DEF CON this year, whether you're attending virtually or here with us in Las Vegas. DEF CON "U. Tomorrow it begins!

## Get the DEF CON 29 Soundtrack!

Posted 8.4.21

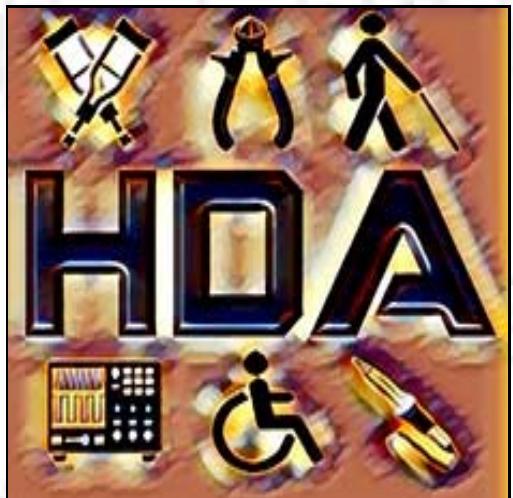


Get a head start on DEF CON 29 with this year's Original Soundtrack! It's waiting for you on the DEF CON media server right now. Like, right now. You have your assignment.

[media.defcon.org/DEF CON 29/](http://media.defcon.org/DEF CON 29/)

## Hackers with Disabilities Guide for DEF CON 29!

Posted 8.2.21



Thanks to [@A\\_P\\_Delchi](#) and Hackers with Disabilities for creating this helpful [accessibility guide to DC29](#). Don't hesitate to reach out if we can help maximize your DEF CON, either through goons or via social media.

---

[Return to Index](#)

# DEF CON 30 FAQ

---

## FREQUENTLY ASKED QUESTIONS

---

When & Where will DEF CON be?

Aug. 11-14, 2022 at Caesars Forum + Flamingo, Harrah's and Linq in Las Vegas!

---

Can I book my hotel in Las Vegas now – and how should I do that?

Yes, hotel reservations are being accepted. In order to help us fill our room block with our contracted hotels please book under the [DEF CON group room registration](#).

---

What is DEF CON doing for DC30, and how can I attend?

DEF CON 30 will be a semi-hybrid event this year, we will give hackers a choice in how they wish to experience DEF CON but we are returning at full operating capacity. What do we mean by semi-hybrid? We will be hosting our full con in-person in Las Vegas and our approved villages and contests will be contributing additional online content within the official DEF CON Discord. All Online content will be similar to the 2020 & 2021 cons. Our official talks will be streamed via DCTV on our Twitch, and several contests and villages will be providing unique online immersive contests and presentations.

To see what happenings are currently planning to be in-person, hybrid, or virtual only please visit  
<https://forum.defcon.org/node/239768>

---

How much will DEF CON cost?

The price to attend DEF CON in-person will be \$360 USD. You may not attend in-person without purchasing a badge. Attending virtual on our Discord will be free, and those with Human+ will have more permissions and access.

You can support DEF CON and upgrade your account by purchasing the [Human Plus](#) role.

---

Can I register for in-person DEF CON online?

Update: Online sales have closed. DC 30 badges can now be purchased with cash at the door.

Yes. DEF CON is a cash-at-the-door kind of conference. Paying in cash helps protect your privacy, and search warrants can't vacuum up PII we don't collect. You will always be able to lay down US dollars in the reg line and collect your badge. Still, the experience of DC29 taught us a few things. Some of our attendees work DEF CON into their business travel schedule, and the option to pre-reg with a credit card over the web made things much easier for them. Some of our attendees need to manage a group purchase, or want a more detailed receipt.

For everyone who fits into those categories, we're happy to announce that we're keeping the option of online registration. You'll be able to use [shop.defcon.org](https://shop.defcon.org) to buy your ticket and get your receipt. We hope the online option makes the process more streamlined for those who need it. We thank people for their patience and feedback as we navigate the changing landscape. The price for DEF CON 30 is \$360, with a processing fee of \$9.66 added to online orders.

---

Can I buy a DEF CON badge with Black Hat?

Yes, it will be an option when you check out at Black Hat.

---

How do I participate in virtual DEF CON?

**For the virtual portion of DEF CON you will need a Discord account.**

You can find detailed [instructions on getting on the DEF CON Discord server here](#). There is a [FAQ for Humans on Discord](#) as well.

You can support DEF CON and upgrade your account by purchasing the [Human Plus](#) role that gives you more permissions than the free "Human" role. Connect to the DEF CON Discord Server: <https://discord.gg/DEFCON>

To see what happenings are currently planning to be in-person, hybrid, or virtual only please visit <https://forum.defcon.org/node/239768>

---

What if I don't want a Discord Account?

While we don't think you'll get the full experience, all of our content will be released via YouTube and put on the DEF CON Media Server. The Talks for DEF CON will be released during the con on the [DEF CON YouTube](#) and [Twitch](#) channels.

---

Will there be Uber Badges again?

Our annual tradition of awarding black "Uber" badges for CTF and other select contests, will continue, for in-person events only. To make sure that attendees are playing contests with the full hacker spirit we don't announce which contests qualify for an Uber Badge ahead of the contest (aside from the Official CTF) . We want to see how well each contest operates, and how players perform, so those decisions aren't made until Sunday of the con. Check out the registry of past [black badge winners!](#)

---

Where can I find more info on the DEF CON CTF?

DEF CON CTF Qualifiers May 28-29. Please follow Nautilus CTF on twitter at [https://twitter.com/Nautilus\\_CTF](https://twitter.com/Nautilus_CTF) and keep a look out on their CTF website at <https://nautilus.institute>. For a little history on the contest check out the [CTF History](#) page.

---

I have a black badge, do I need to pre-register?

No, just show up on site and go to inhuman registration. The rules governing the use of Black Badges are available on the [Black Badge Policy Page](#). If you notice any errors or omissions in the list, please contact us at [info@defcon.org](mailto:info@defcon.org). Congratulations to everyone who's earned a Black Badge and good luck to all who seek one.

---

What will capacity look like for the in-person event?

Capacity is currently capped at each given space's fire code standard capacity. In case of changing health and safety recommendations, limits will be reviewed and revised at the direction of Southern Nevada Health District (SNHD) and there will be dedicated support onsite to ensure our policies are being followed.

---

What health measures/protocols is DEF CON taking to ensure a safe environment on-site?

DEF CON is working closely with Caesars Entertainment hotels to provide a safe and healthy experience for all. We will comply with whatever safety measures are required of us.

---

Will I be required to wear a mask?

Yes. Barring a major change in the situation, we will not check proof of vaccination, but we will keep last year's mask requirement in place for DEF CON 30. Protecting the community is our first priority, and we want to make sure that everyone is as safe as we can make them. *Everyone* includes the healthy, the vulnerable and those who have immune compromised loved ones they need to protect.

Thank you for all you did to protect each other last year, and with your help we'll do it again this year.

---

What's DEF CON's official theme for DEF CON 30?

We want DEF CON 30 to have the energy of a reunion. We'll be back together in a brand spanking new venue. We'll be thirty years old - an amazing milestone for a hacker conference under any circumstances. In honor of all that, we're calling DEF CON 30 'Hacker Homecoming'. More info on our official theme is here:  
<https://defcon.org/html/links/dc-news.html#dc30theme>

---

Where can I get more information about what's happening?

Check out the following DEF CON Sites & Social Media.

[Forums](#)

[Groups](#)

[Discord](#)

[Twitter](#)

[Facebook](#)

[Reddit](#)

[DEF CON YouTube channel](#)

[DEF CON Twitch](#)

[DEF CON Music Twitch](#)

[DEF CON Media Server of all past conference materials](#)

---

[Return to Index](#)

---

© 1992-2022 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 were 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 30 will be held August 11th through August 14th. We are gauging interest on what degree of where. 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 can be found at <http://defcon.stotan.org/faq/>

---

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](#) (call for papers). 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\[at\]defcon\[d0t\]org](mailto:press[at]defcon[d0t]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.

---

## How much is admission DEF CON, and do you take credit cards?

The price for DEF CON 30 is USD\$360 cash at the door. We do this for a number of reasons. Paying in cash protects your privacy and we can't be forced to hand over records we don't collect. Still, offering online registration for DEF CON Safe Mode taught us we had some attendees who really benefit from the option for things like group orders and expense report requirements.

For those attendees who need a credit card option we'll continue to offer online ticket sales at [shop.defcon.org](http://shop.defcon.org). There is a \$9.66 processing fee for these online transactions. We hope this makes things easier for the community members who need it.

---

## 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.

Along with your request, please email us the following to info(at)defcon(.)org

Name as is on passport:

Passport number:

Country of issue:

Date of issue:

Date of expiration:

Country of origin:

---

DEF CON is too expensive, how can I afford it?

DEF CON is cheaper than many concerts, and certainly cheaper than many shows in Vegas. 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?

The DEF CON 30 group room registration is now live! We have room rates at seven hotels, until they run out of rooms in our block.

Follow this link: <https://book.passkey.com/go/SHDEF2>

Do not worry if the form doesn't immediately show the discounted rate. To verify that you're getting our price you can mouse over the dates you've selected or begin the checkout process.

---

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, and a couple of tracks out to the internet, for several years now. We don't expect this will change!

---

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. The hotel is 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.

---

[Return to Index](#)

---

# Links to DEF CON 30 related pages

---

## Maps

- Overview around DEF CON 30
- ◆ Harrahs Full map
- ◆ Linq Full map
- ◆ Flamingo Full map
  - ◊ Flamingo Lower Level
  - ◊ Flamingo Third Floor
- ◆ Caesars Forum Full map
  - ◊ Caesars Forum Forum BR
  - ◊ Caesars Forum Summit BR
  - ◊ Caesars Forum Academy BR
  - ◊ Caesars Forum Alliance BR
  - ◊ 3D tour of Caesars Forum, like Google StreetView

## Links

### DEF CON . org

Main DEF CON site

DEF CON 30 Home Page

DEF CON FAQ

DEF CON 30 FAQ

DEF CON Recent News

DEF CON Venue

DEF CON 30 Schedule

DEF CON 30 Entertainment

DEF CON 30 Policy

DEF CON 30 Training Home

DEF CON 30 Training List

DEF CON CTF Nautilus Institute, Twitter [@Nautilus\\_CTF](#)

DEF CON YouTube channel, prev years talks

DEF CON Forum Calendar

DEF CON 30 Planning Forum page

DEF CON 30 Speakers & Presentations Forum page

DEF CON 30 Villages Forum page

DEF CON 30 Contests Forum page

DEF CON 30 Parties & Gatherings & Events Forum page

DEF CON 30 Demolabs Forum page

DEF CON 30 Workshops Forum page - Registration opened on July 5 at Noon PDT! - All Workshops are Sold Out!

DEF CON 30 Paid Training Forum page - These occur the 2 days following DEF CON

---

Thanks to the InfoBooth crew for providing access to their backend database. <claps> to their hard work!

---

### Villages Info

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

You may need to scroll to the right to see all info

Village Name Home Page	Map	Schedule	Forum Link	Social Media Links
Adversary Village	<a href="#">Map</a>	<a href="#">Sched</a>	<a href="#">Forum</a>	TW @AdversaryVillag IG @AdversaryVillage LI @adversaryvillage FB @AdversaryVillage TI @AdversaryVillage DC <a href="https://discord.gg/GDB3rC7KYz">https://discord.gg/GDB3rC7KYz</a> YT link
Aerospace Village	<a href="#">Map</a>	<a href="#">Sched</a>	<a href="#">Forum</a>	TW @secureaerospace LI @aerospace-village TW @hack_a_sat DC <a href="https://discord.gg/gV4EWuk">https://discord.gg/gV4EWuk</a>
AppSec Village	<a href="#">Map</a>	<a href="#">Sched</a>	<a href="#">Forum</a>	TW @AppSec_Village LI @appsecvillage YT <a href="https://www.youtube.com/c/AppSecVillage">https://www.youtube.com/c/AppSecVillage</a>
Artificial Intelligence Village	<a href="#">Map</a>	<a href="#">Sched</a>	<a href="#">Forum</a>	TW @aivillage_dc TI @aivillage YT link DC <a href="https://discord.com/invite/GX5fhfT">https://discord.com/invite/GX5fhfT</a>
Bio Hacking Village	<a href="#">Map</a>	<a href="#">Sched</a>	<a href="#">Forum</a>	TW @dc_bhv LI @biohacking-village YT <a href="http://youtube.com/biohackingvillage">http://youtube.com/biohackingvillage</a> TI @biohackingvillage DC <a href="https://discord.gg/Q8ubDb5">https://discord.gg/Q8ubDb5</a> SP link
Blacks in Cybersecurity	<a href="#">Map</a>	<a href="#">Sched</a>	<a href="#">Forum</a>	TW @BlackInCyberCo1 IG @blackincyberconf TI @blacksincybersecurity YT link LI @blackincyberconference PT @blacksincybersecurity FB @blackincyberconf
Blue Team Village	<a href="#">Map</a>	<a href="#">Sched</a>	<a href="#">Forum</a>	TW @BlueTeamVillage TI @blueteamvillage YT <a href="https://www.youtube.com/c/blueteamvillage">https://www.youtube.com/c/blueteamvillage</a> DC <a href="https://discord.com/invite/blueteamvillage">https://discord.com/invite/blueteamvillage</a>
Car Hacking Village	<a href="#">Map</a>	<a href="#">Sched</a>	<a href="#">Forum</a>	TW @CarHackVillage DC <a href="https://discord.gg/JWCcTAM">https://discord.gg/JWCcTAM</a>
Cloud Village	<a href="#">Map</a>	<a href="#">Sched</a>	<a href="#">Forum</a>	TW @cloudvillage_dc YT <a href="https://www.youtube.com/cloudvillage_dc">https://www.youtube.com/cloudvillage_dc</a> DC <a href="https://discord.gg/EygUDJABee">https://discord.gg/EygUDJABee</a>
Crypto Privacy Village	<a href="#">Map</a>	<a href="#">Sched</a>	<a href="#">Forum</a>	TW @cryptovillage SL <a href="https://cryptovillage.slack.com/">https://cryptovillage.slack.com/</a> YT link TI @cryptovillage
Data Duplication Village	<a href="#">Map</a>	<a href="#">Sched</a>	<a href="#">Forum</a>	TW @DDV_DC

Village Name Home Page	Map	Schedule	Forum Link	Social Media Links
Girls Hack Village	Map		Forum	TW @girlshackvllg IG @blackgirlshack
Ham Radio Village	Map		Forum	TW @HamRadioVillage TI @HamRadioVillage DC <a href="https://discord.gg/hrv">https://discord.gg/hrv</a>
Hardware Hacking Soldering Skills Village	Map	Sched	Forum	TW @DC_HHV
Industrial Control Systems Village	Map	Sched	Forum	TW @ICS_Village LI @icsvillage YT link TI @ics_village
Internet Of Things Village	Map	Sched	Forum	TW @iotvillage TW @ISEsecurity TW @Villageidiotlab LI @iotvillage TI @iotvillage YT <a href="https://www.youtube.com/c/IoTVillage/videos">https://www.youtube.com/c/IoTVillage/videos</a> DC <a href="https://discord.gg/tmZASSpNnP">https://discord.gg/tmZASSpNnP</a>
Lock Pick Village	Map		Forum	TW @toool TI @toool_us YT <a href="https://youtube.com/c/TOOOL-US">https://youtube.com/c/TOOOL-US</a>
MisInformation Village	Map		Forum	TW @MisinfoVillage TW @misinfocon
Packet Hacking Village	Map	Sched	Forum	TW @wallofssheep FB @wallofssheep YT <a href="https://youtube.com/wallofssheep">https://youtube.com/wallofssheep</a> TI @wallofssheep PS <a href="https://www.periscope.tv/wallofssheep">https://www.periscope.tv/wallofssheep</a>
Password Village	Map	Sched	Forum	TW @PasswordVillage TI @passwordvillage YT link
Payment Village			Forum	TW @paymentvillage TI @paymentvillage YT link
Physical Security Village	Map		Forum	TW @bypassvillage TI @bypassvillage
Policy Village	Map	Sched	Forum	
Quantum Village	Map		Forum	TW @quantum_village
Radio Frequency Village	Map		Forum	TW @rfhackers TW @rf_ctf link DC <a href="https://discordapp.com/invite/JjPQhKy">https://discordapp.com/invite/JjPQhKy</a>
Recon Village	Map	Sched	Forum	TW @ReconVillage FB @reconvillage
Red Team Village	Map	Sched	Forum	TW @RedTeamVillage_ YT <a href="https://www.youtube.com/redteamvillage">https://www.youtube.com/redteamvillage</a> TI @redteamvillage DC <a href="https://discord.gg/redteamvillage">https://discord.gg/redteamvillage</a>
Retail Hacking Village	Map	Sched	Forum	

Village Name Home Page	Map	Schedule	Forum Link	Social Media Links
				TW @RetailHacking DC <a href="https://discord.gg/DxG4Uj7WZV">https://discord.gg/DxG4Uj7WZV</a>
Rogues Village	Map	Sched	Forum	TW @RoguesVillage TI @roguesvillage TW @foursuits_co YT <a href="https://www.youtube.com/c/foursuits">https://www.youtube.com/c/foursuits</a>
SkyTalks - 303	Map	Sched	Forum	TW @dcskytalks FB @Skytalks
Social Engineering Village	Map	Sched	Forum	TW @sec_defcon
Tamper Evident Village	Map		Forum	
Voting Machine Village	Map		Forum	TW @votingvillagedc YT link

## DEF CON 30 Speakers & Presentations

DEF CON 30 [Schedule](#)

DEF CON 30 All Speakers [Forum page](#)

DEF CON only!, no villages

## Combined Schedules of DEF CON, Villages, and everything else DC30

At this time these have no content

Hacker Tracker - [Android](#) and [IOS](#) - the official DEF CON schedule app

The ONE! - A consolidated DEFCON 30 schedule in multiple file formats - html, PDF, CSV, ICAL, epub, mobi, Google calendar

[info.defcon.org](http://info.defcon.org) - the official DEF CON InfoBooth site

## Contests Info

Various contests, some lasting all 4 days of DEF CON, some short time on stage

One Page [All Contests](#) list with descriptions

DEF CON 30 All Contests [Forum page](#)

You may need to scroll to the right to see all info

Alpac@tack <a href="#">Contest Info</a>	Auto Driving CTF <a href="#">Contest Info</a>
Betting on Your Digital Rights: EFF Benefit Poker Tournament <a href="#">Contest Info</a>	Beverage Cooling Contraption Contest <a href="#">Contest Info</a>
Capture The Packet <a href="#">Contest Info</a>	Car Hacking CTF <a href="#">Contest Info</a>
CMD+CTRL at DEF CON 30 <a href="#">Contest Info</a>	Crack Me If You Can <a href="#">Contest Info</a>

<a href="#">Crash and Compile Contest Info</a>	<a href="#">Creative Writing Short Story Contest Contest Info</a>
<a href="#">Darknet-NG Contest Info</a>	DEF CON 30 Chess Tournament. <a href="#">Contest Info</a>
<a href="#">DEF CON Capture the Flag Contest Info</a>	DEF CON Kubernetes Capture the Flag (CTF) <a href="#">Contest Info</a>
<a href="#">DEF CON MUD Contest Info</a>	DEF CON Red Team CTF <a href="#">Contest Info</a>
<a href="#">DEF CON Scavenger Hunt Contest Info</a>	DEF CONs Next Top Threat Model <a href="#">Contest Info</a>
<a href="#">Defcon Ham Radio Fox Hunting Contest Contest Info</a>	EFF Tech Trivia <a href="#">Contest Info</a>
<a href="#">Hack Fortress Contest Info</a>	Hack the Plan[e]t <a href="#">Contest Info</a>
<a href="#">Hack3r Runw@y Contest Info</a>	Hacker Jeopardy <a href="#">Contest Info</a>
<a href="#">Hospital Under Seige Contest Info</a>	IoT CTF Creators Challenge <a href="#">Contest Info</a>
<a href="#">IoT Village Hacking CTF Contest Info</a>	Octopus Game <a href="#">Contest Info</a>
<a href="#">Packet Detective &amp; Packet Inspector Contest Info</a>	pTFS Presents: Mayhem Industries – Outside the Box <a href="#">Contest Info</a>
<a href="#">Radio Frequency Capture the Flag Contest Info</a>	Red Alert ICS CTF <a href="#">Contest Info</a>
<a href="#">SE Community (SEC) Vishing Competition / #SECVIC Contest Info</a>	Social Engineering Community (SEC) Youth Challenge <a href="#">Contest Info</a>
<a href="#">Sticker Design Contest Contest Info</a>	The BIC Village Capture the Flag <a href="#">Contest Info</a>
<a href="#">The Gold Bug Contest Info</a>	The Hack-n-Attack Hacker Homecoming Heist <a href="#">Contest Info</a>
<a href="#">The Schemaverse Championship Contest Info</a>	The TeleChallenge <a href="#">Contest Info</a>
<a href="#">Tin Foil Hat Contest Contest Info</a>	Trace Labs OSINT Search Party CTF <a href="#">Contest Info</a>
<a href="#">Whose Slide Is It Anyway Contest Info</a>	

## Demolabs Info

Brief demonstrations for people to show off their project.

One Page [All Demolabs](#) list with descriptions  
 DEF CON 30 All Demolabs [Forum page](#)

You may need to scroll to the right to see all info

AADInternals: The Ultimate Azure AD Hacking Toolkit - Nestori Syynimaa  
[Demolabs Info](#)

Access Undenied on AWS - Noam Dahan

[Demolabs Info](#)

alsanna - Jason Johnson

[Demolabs Info](#)

AWSGoat: A Damn Vulnerable AWS Infrastructure - Jeswin, Sanjeev

[Demolabs Info](#)

AzureGoat: Damn Vulnerable Azure Infrastructure - Nishant, Rachna Learn/teach/practice Azure pentesting.

[Demolabs Info](#)

Badrats: Initial Access Made Easy - Kevin, Dominic

[Demolabs Info](#)

Control Validation Compass – Threat Modeling Aide & Purple Team Content Repo - Scott Small

[Demolabs Info](#)

CyberPeace Builders - Adrien Ogee

[Demolabs Info](#)

Defensive 5G - Eric Mair, Ryan Ashley A 4.5G/5G test infrastructure using COTS hardware and OS software.

[Demolabs Info](#)

EDR detection mechanisms and bypass techniques with EDRSandBlast - Thomas Diot, Maxime Meignan

[Demolabs Info](#)

EMBA - Open-Source Firmware Security Testing - Messner, Eckmann

[Demolabs Info](#)

Empire 4.0 and Beyond - V. Rose, A. Rose

[Demolabs Info](#)

FISSURE: The RF Framework - Christopher Poore

[Demolabs Info](#)

hls4ml - Open Source Machine Learning Accelerators on FPGAs - Hawks, Meza

[Demolabs Info](#)

Injectyll-HIDe: Pushing the Future of Hardware Implants to the Next Level - Fischer, Miller

[Demolabs Info](#)

Memfini - A systemwide memory monitor interface for linux - Shubham Dubey, Rishal Dwivedi

[Demolabs Info](#)

Mercury - David McGrew, Brandon Enright

[Demolabs Info](#)

OpenTDF - Paul Flynn, Cassandra Bailey

[Demolabs Info](#)

Packet Sender - Dan Nagle

[Demolabs Info](#)

PCILeech and MemProcFS - Ulf Frisk, Ian Vitek

[Demolabs Info](#)

PMR - PT & VA Management & Reporting - Alanazi, Bin Muatred

[Demolabs Info](#)

ResidueFree - Logan Arkema

[Demolabs Info](#)

SharpSCCM - Chris Thompson, Duane Michael

[Demolabs Info](#)

svachal + machinescli - Ankur Tyagi

[Demolabs Info](#)

TheAllCommander - Matthew Handy

[Demolabs Info](#)

unblob - towards efficient firmware extraction - Kaiser, Lukavsky

[Demolabs Info](#)

Vajra - Your Weapon To Cloud - Raunak Parmar

[Demolabs Info](#)

Wakanda Land - Stephen Kofi Asamoah

[Demolabs Info](#)

Xavier Memory Analysis Framework - Solomon Sonya

[Demolabs Info](#)

Zuthaka: A Command & Controls (C2s) integration framework - Lucas Bonastre, Alberto Herrera

[Demolabs Info](#)

## Workshops Info

Longer, more detailed, hands on, lasting half a day.

These have limited seating.

Workshop Registration Opened July 5 Noon PDT - All Workshops are Sold Out!

[EventBrite DEF CON Workshops signup page](#)

One Page [All Workshops](#) list with descriptions

DEF CON 30 All Workshops [Forum page](#)

You may need to scroll to the right to see all info

SOLD OUT - Creating and uncovering malicious containers - Adrian Wood, David Mitchell, and Griffin Francis  
[Workshop Info](#)

SOLD OUT - Evading Detection: A Beginner's Guide to Obfuscation - Anthony Rose, Jake "Hubbl3" Krasnov, Vincent "Vinnybod" Rose

[Workshop Info](#)

SOLD OUT - Pentesting Industrial Control Systems 101: Capture the Flag! - Arnaud Soullie, Alexandrine Torrents  
[Workshop Info](#)

SOLD OUT - Securing Industrial Control Systems from the core: PLC secure coding practices - Arnaud Soullie, Alexandrine Torrents

[Workshop Info](#)

SOLD OUT - Pivoting, Tunneling, and Redirection Master Class - Barrett Darnell, Wesley Thurner

[Workshop Info](#)

SOLD OUT - Hands-On TCP/IP Deep Dive with Wireshark - Chris Greer

[Workshop Info](#)

SOLD OUT - CTF 101: Breaking into CTFs... - Christopher Forte, Robert Fitzpatrick

[Workshop Info](#)

SOLD OUT - Hacking the Metal 2: Hardware and the Evolution of C Creatures - Eigentourist

[Workshop Info](#)

SOLD OUT - Dig Dug: The Lost Art of Network Tunneling - Eijah, Cam

[Workshop Info](#)

SOLD OUT - Protect/hunt/respond with Fleet and osquery - Guillaume Ross, Kathy Satterlee

[Workshop Info](#)

SOLD OUT - Finding Security Vulnerabilities Through Fuzzing - Hardik Shah

[Workshop Info](#)

SOLD OUT - Hybrid Phishing Payloads: From Threat-actors to You - Jon Christiansen, Magnus Stubman  
[Workshop Info](#)

SOLD OUT - The Art of Modern Malware Analysis - Josh Stroschein, Ryan J Chapman, Aaron Rosenmund  
[Workshop Info](#)

SOLD OUT - Introduction to Cryptographic Attacks - Matt Cheung  
[Workshop Info](#)

SOLD OUT - The Purple Malware Development Approach - Mauricio Velazco, Olaf Hartong  
[Workshop Info](#)

SOLD OUT - House of Heap Exploitation - Maxwell Dulin, Zachary Minneker, Kenzie Dolan, Justin drtychai Angra  
[Workshop Info](#)

SOLD OUT - DFIR Against the Digital Darkness: An Intro to Forensinating Evil - Michael Solomon, Michael Register  
[Workshop Info](#)

SOLD OUT - Introduction to Azure Security - Nishant Sharma, Jeswin Mathai  
[Workshop Info](#)

SOLD OUT - Hand On Mainframe Buffer Overflows - Phil Young, Jake Labelle  
[Workshop Info](#)

SOLD OUT - CICD security: A new eldorado - Remi Escourrou, Xavier Gerondeau, Gauthier Sebaux  
[Workshop Info](#)

SOLD OUT - Introduction to Software Defined Radios and RF Hacking - Rich  
[Workshop Info](#)

SOLD OUT - Windows Defence Evasion and Fortification Primitives - Rohan Durve, Paul Laîné  
[Workshop Info](#)

SOLD OUT - FROM ZERO TO HERO IN A BLOCKCHAIN SECURITY - Roman Zaikin, Dikla Barda, Oded Vanunu  
[Workshop Info](#)

SOLD OUT - Securing Web Apps - Sam Bowne, Elizabeth Biddlecome, Irvin Lemus, Kaitlyn Handelman  
[Workshop Info](#)

SOLD OUT - Securing Smart Contracts - Sam Bowne, Elizabeth Biddlecome, Irvin Lemus, Kaitlyn Handelman  
[Workshop Info](#)

SOLD OUT - Automated Debugging Under The Hood... - Sergei Frankoff, Sean Wilson  
[Workshop Info](#)

SOLD OUT - Master Class: Delivering a New Construct in Advanced Volatile Memory Analysis for Fun and Profit - Solomon Sonya  
[Workshop Info](#)

SOLD OUT - Network Hacking 101 - Victor Graf and Ben Kurtz  
[Workshop Info](#)

## Paid Training Info

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 30 All Paid Training [Forum page](#)  
DEF CON 30 Training [Signup Pages](#)

You may need to scroll to the right to see all info

Defender's Guide to Securing Public Cloud Infrastructures - Abhinav Singh  
[Paid Training Info](#)

Pragmatic API Exploration - Aubrey Labuschagne (William) & Marianka Botes

[Paid Training Info](#)

TCP/IP Deep Dive for Ethical Hackers – Featuring Wireshark - Chris Greer

[Paid Training Info](#)

Zero 2 Emulated Criminal: Intro to Windows Malware Dev - Dahvid Schloss

[Paid Training Info](#)

Customizable Binary Analysis: Using angr to its full potential - Fish Wang & Audrey Dutcher

[Paid Training Info](#)

A Practical Approach to Breaking & Pwning Kubernetes Clusters - Madhu Akula

[Paid Training Info](#)

- Offensive IoT Exploitation

[Paid Training Info](#)

Practical Secure Code Review - Seth Law & Ken Johnson

[Paid Training Info](#)

---

## Open Calls

Village	Call For Info
AI Village	<a href="#">Twitter Call 4 Volunteers</a>
303/SkyTalks Village	<a href="#">Twitter Call 4 Volunteers</a>
Blue Team Village	<a href="#">Twitter Call 4 Volunteers</a>
Crypto & Privacy Village	<a href="#">Twitter Call 4 volunteers</a>
Data Duplication Village	<a href="#">Call for Volunteers</a>
DC Groups VR Event	<a href="#">Twitter Call 4 Submissions</a> , closes July 15
Lock Pick Village	<a href="#">Twitter Call 4 Content</a>
Physical Security Village	Calls for <a href="#">Proposals</a> , <a href="#">Exhibits</a> , <a href="#">Volunteers</a> , closes July 16 <a href="#">Twitter call 4 Papers</a> , <a href="#">Exhibits</a> , <a href="#">Volunteers</a> <a href="#">Twitter Volunteer Perks</a> <a href="#">Twitter call 4 Displays</a>
Quantum Village	<a href="#">Twitter call 4 Participation</a>
Recon Village	<a href="#">Twitter call 4 Volunteers</a>
Red Team Village	<a href="#">Twitter call 4 Volunteers</a> <a href="#">Twitter call 4 Workshops</a> <a href="#">Twitter call 4 Sponsors</a>
Retail Hacking Village	Calls for <a href="#">Talks</a> , <a href="#">Staff</a>

---

## Villages Waiting for Calls or no Calls

Internet Of Things Village

Packet Hacking Village

Password Village

Payment Village

Policy Village

Tamper Evident Village

---

## Villages with Completed Calls

DEF CON Call for [Papers](#) closed May 1  
DEF CON Call for [Demo Labs](#) closed May 1  
DEF CON Call for [Workshops](#) closed May 1  
DEF CON Call for [Parties & Meetups](#) closed April 30  
DEF CON Call for [Training](#) closed May 16  
DEF CON Call for [Music](#) closed June 1  
303 / SkyTalks Call for [Presentations](#) closed May 31  
Adversary Village [Call For Papers](#) closed May 15  
Aerospace Village [Call For Everything](#) closed June 3  
AppSec Village [Call For Papers](#) closed May 10  
Artificial Intelligence Village [Twitter Call 4 Papers](#) closed June 22  
Bio Hacking Village calls for [Equipment, Papers, Workshops](#) closed April 30  
Blacks in Cybersecurity [Call for papers](#) closed June 1  
Blue Team Village Call for [Content](#) closed May 15  
Car Hacking Village [Twitter Call 4 Papers](#) closed June 24  
Cloud Village Call for [Papers, Volunteers, Sponsors](#) closed June 5  
Crypto & Privacy Village Call for [Presentations and Workshops](#) closed June 26  
Data Duplication Village [Call for Papers](#) closed June 26  
Girls Hack Village [Call for proposal](#) closed June 15  
Ham Radio Village Calls for [Papers Staff VEs](#) closed July 24  
Hardware Hacking and Soldering Skills Village Calls for [Papers and Volunteers](#) closed June 17  
Industrial Control Systems ( ICS ) Village [Twitter Call 4 Papers](#) closed June 24  
MisInformation Village [Call for Proposals](#) closed July 3  
Radio Frequency Village [Twitter call 4 Papers](#) closed July 4  
Recon Village [Twitter call 4 Papers](#) closed June 27  
Rogues Village Call for [Papers](#) closed June 30  
Social Engineering Village Calls, [CFP](#), [CFC](#), [CFV](#), [CFR](#) closed June 3, June 3, June 3, July 1  
Voting Machine Village [Twitter call 4 Papers](#) closed June 13

---

## Non-Village Call Fors

DCFurs 2022 website - [Call For Presentations](#)  
[Mental Health Hackers](#) and their [Call for Papers](#)  
[@defcongroups](#) VR Event, Twitter [Call For VR Talks](#)  
BlanketFortCON Twitter [Call for DJs](#)

---

## Other Interesting Links

[@defconparties](#) - calendar  
[defconmusic](#) - Schedule/News from the DC Artists & Entertainment ( A&E ) Department  
[defcon](#) [DEFCONorg](#) Twitch stream  
[defconmusic](#) DEF CON Entertainment Twitch stream  
[defconmusic](#) YouTube channel  
[#badgelife](#) spreadsheet of unofficial badges for DC30  
[@qumqats](#) Twitter [List of Village](#) accounts to assist in watching Village happenings

Other cons during #SummerHackerCamp

Blackhat	T <a href="#">@BlackHatEvents</a>	FB <a href="#">Black Hat Events</a>
BSides Las Vegas	T <a href="#">@BSidesLV</a>	FB <a href="#">@BSidesLV</a>
Queercon	T <a href="#">@Queercon</a>	FB <a href="#">@queercon</a>
The Diana Initiative	T <a href="#">@Dianainitiative</a>	FB <a href="#">@dianainitiative</a>

## Guides/Tips/FAQs

[OpSec For DEF CON 30](#)

[DCG 201 Hacker Double Summer 2022 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](#)

---

Thanks for your interest in this post/page. I hope it was useful to you.

Production of this post/page is not affiliated with DEFCON 30.

Use at your own risk.

For the latest info while at DC30 please check the info booths and screens.

If you notice any problems or something is missing in this post/page please let me know. Constructive comments and additional info is welcome.

Have a good DEFCON 30!

email: [qumqats@outel.org](mailto:qumqats@outel.org)

Twitter: [@qumqats](#)

---